

Data Protection & Privacy

Jurisdictional comparisons

First edition 2012

Preface Monika Kuschewsky Van Bael & Bellis

Foreword Viviane Reding, Vice-President of the European Commission, Commissioner for Justice, Fundamental Rights and Citizenship

Foreword Peter Hustinx, European Data Protection Supervisor

Foreword Jean Gonié, Director of Privacy, EU Affairs, Microsoft Europe

Austria Dr Rainer Knyrim Preslmayr Rechtsanwälte OG

Belgium Monika Kuschewsky Van Bael & Bellis

Canada David Elder Stikeman Elliott LLP

Cyprus Nicholas Ktenas & Chrystalla Neophytou Andreas Neocleous & Co LLC

Czech Republic Richard Otevřel Havel, Holásek & Partners

Denmark Johnny Petersen DELACOUR DANIA

EU Monika Kuschewsky Van Bael & Bellis

France Raphaël Dana & Ramiro Tavella Sarrut Avocats

Germany Monika Kuschewsky Van Bael & Bellis

Hungary János Tamás Varga & Zoltán Tarján VJT & Partners Law Firm

India Naheed Carrimjee Desai Desai Carrimjee & Mulla

Israel Yoheved Novogroder-Shoshan Yigal Arnon & Co

Italy Gerolamo Pellicanò & Giovanna Boschetti CBA Studio Legale e Tributario

Latvia Linda Lejina & Ilze Bukaldere BORENIUS

Luxembourg Héloïse Bock Arendt & Medernach

Malta Michael Zammit Maempel & Mark Hyzler GVTH Advocates

Mexico Laura Collada & Jorge Molet Dumont Bergman Bider & Co., S.C.

Netherlands Polo van der Putt & Eva de Vries Vondst Advocaten

Poland Agata Szeliga Sołtysiński, Kawecki & Szlęzak

Portugal Mónica Oliveira Costa Coelho Ribeiro e Associados

Republic of Ireland Jeanne Kelly & Aoife Treacy Mason, Hayes & Curran

Romania Roxana Ionescu & Ovidiu Balaceanu Nestor Nestor Diculescu Kingston Petersen

Slovakia Richard Otevřel & Jaroslav Šuchman Havel, Holásek & Partners

South Africa André Visser & Danie Strachan Adams & Adams

Spain Cecilia Álvarez Rigaudias & Leticia López-Lapuente Uría Menéndez

Sweden Erica Wiking Häger, Mikael Moreira & Anna Nidén Mannheimer Swartling

Switzerland Dr Lukas Morscher & Martin Vonaesch Lenz & Staehelin

Turkey Gönenç Gürkaynak, İlay Yılmaz & Ceren Yıldız ELIG Attorneys at Law

UK Hazel Grant & Mark Watts Bristows

USA Andrew Serwin, Daniel Muto & Megan O'Sullivan Foley & Lardner

General Editor: Monika Kuschewsky
Van Bael & Bellis

THE EUROPEAN LAWYER
REFERENCE

Israel

Yigal Arnon & Co Yoheved Novogroder-Shoshan¹

1. LEGISLATION

1.1 Name\title of the law

The Protection of Privacy Law 1981 (Privacy Law) is the main Israeli law dealing with the collection and use of personal data. The Privacy Law is supplemented by various regulations, including:

- Protection of Privacy Regulations (Determination of Databases Containing Non-Disclosable Data) 1987;
- Protection of Privacy Regulations (Conditions for Possessing and Protecting Data and Procedures for Transferring Data Between Public Bodies) 1986 (Data Possession Regulations);
- Protection of Privacy Regulations (Conditions for Inspection of Data and Procedures for Appeal from a Denial of a Request to Inspect) 1981 (Data Inspection Regulations);
- Protection of Privacy Regulations (Fees) 2000;
- Administrative Offences Regulations (Administrative Fine – Protection of Privacy) 2004;
- Protection of Privacy Regulations (Transfer of Information to Databases outside of the State's Boundaries) 2001 (Data Transfer Regulations);
- Protection of Privacy Order (Determination of Public Bodies) 1986;
- Protection of Privacy Order (Determination of the Investigatory Authority) 1998;
- Protection of Privacy Order (Establishment of Regulatory Unit) 1999.

The right to privacy is recognised as a fundamental human right under the quasi-constitutional Basic Law: Human Dignity and Liberty, which provides that: *'every person is entitled to privacy and to the confidentiality of his life' and 'there shall be no infringement of the confidentiality of a person's conversations, correspondence and writings'*.

In addition, certain sector-specific laws provide additional protection for the types of information referenced in such laws. Among these are the Patients' Rights Law 1996 (medical information); Genetic Information Law 2000 (genetic information); the Psychologists' Law 1977 (information disclosed in the context of psychological treatment); the Banking Ordinance 1941 (financial data); and the Credit Information Service Law 2002 (credit information).

Unless otherwise specifically set forth to the contrary below, the responses relate to the Privacy Law as supplemented by complementary regulations and case law.

¹ The author is grateful to Miriam Friedmann for her assistance in preparing this chapter.

1.2 Pending legislation

Two major pieces of legislation are pending. The draft Protection of Privacy Law (Authority of Enforcement) 2010 would amend the existing provisions of the Privacy Law to grant the Registrar of Databases (Registrar) additional investigatory, supervisory and enforcement powers, including the power to impose fines that are substantially higher than those currently authorised under the Privacy Law. The intention is to enable the Registrar to exercise certain powers that are currently held only by the criminal enforcement authorities.

The draft Protection of Privacy Regulations (Information Security in Databases) 2010, if enacted, would impose additional obligations in respect of data security (including relating to physical security requirements, access controls, outsourcing, data destruction and maintenance of backup files) and would require the performance of risk assessments under certain circumstances.

1.3 Scope of the law

The Privacy Law establishes guidelines for the protection of privacy in general, as well as guidelines relating to databases. Personal information not held in a database (as defined under the Privacy Law (see section 1.3.2 below)) is not regulated by the Privacy Law's database provisions, but such information may be used only subject to the Privacy Law's general privacy provisions. Many activities involving database information can also result in civil and criminal liability for invasion of privacy.

Section 2 of the Privacy Law lists 11 activities which constitute an infringement of privacy if they are performed without consent. A number of these activities are relevant to data protection, such as:

- copying a letter or electronic message not intended for publication or using its contents without the permission of the sender or the recipient, provided that the letter or electronic message does not have historic value and 15 years have not passed from the date it was written;
- infringing an obligation of secrecy laid down by law in respect of a person's private affairs;
- using, or passing on to another, information on a person's private affairs, other than for the purpose for which it was given;
- publishing or passing on anything that was obtained by way of an infringement of privacy under certain provisions of the Privacy Law;
- infringing an obligation of secrecy laid down by explicit or implicit agreement in respect of a person's private affairs; and
- publishing any matter that relates to a person's intimate life, state of health or conduct in the private domain.

Section 2 of the Privacy Law also prohibits spying on or trailing a person in a manner likely to harass him, or any other harassment; this prohibition may be relevant in certain contexts in which privacy issues are implicated, such as online behavioural monitoring or use of location data.

This chapter addresses only the regulation of databases.

1.3.1 The main players

The Privacy Law governs the use of database information by any person or entity.

The Privacy Law does not use the term ‘data subject’, however, the definitions of ‘person’, ‘data’ and ‘database’ indicate that the Privacy Law’s database provisions apply only to databases containing information about natural persons. In addition, the rights of inspection and correction of database information (which are discussed more fully below) are accorded solely to natural persons. The Privacy Law does not require that the individual be a resident or citizen of Israel.

It should be noted that while the definition of ‘person’ for the purposes of determining what constitutes an ‘infringement of privacy’ indicates that only an individual’s privacy is protected by the Privacy Law, case law indicates that notwithstanding the definition in the law, corporations may, to some extent, be entitled to protectable privacy rights under the Privacy Law (Civ Petition 1614/02, in Civ File 2324/01 *Multilock Ltd v Rav Bariach Hashkaot Ltd* Tak-Mehozi 2002 (1) 851) and under the Basic Law (Civ File 10434/96 *Keisarit v Ararat* Tak-Mehozi 2000 (3) 26643). Therefore, although the law in this respect is not settled, it appears that the privacy rights of legal persons, although generally thought not to exist, may be afforded some protection under Israeli law.

The Privacy Law identifies three primary actors in connection with databases:

‘Database owner’ is not defined in the Privacy Law. A note on the draft Protection of Privacy Regulations (Information Security in Databases) 2010 compares the role of the database owner to that of the European ‘data controller’, however, the Privacy Law does not state as a general rule that the database owner is primarily responsible for data protection compliance, and allocation of responsibility between database owners and holders is as set forth in the Privacy Law provisions, many of which are described in this chapter.

‘Database holder’ is defined as a person who has a database in his possession on a permanent basis and is permitted to use it.

‘Database manager’ is defined as the active manager of the legal entity which owns or possesses a database, or a person authorised to carry on such activities by the manager for this purpose.

1.3.2 Types of data

‘Data’ are defined as details regarding a person’s personality; personal status; private affairs; state of health; economic situation; professional qualifications; opinions; and faith. The Supreme Court has indicated a willingness to interpret the term ‘data’ broadly, and the term ‘private affairs’ is often construed by Israeli courts as encompassing various types of personal information that are not specifically mentioned in the definition above. For example, Supreme Court decisions have held that individuals’ addresses, telephone numbers, bank account information national ID numbers, and IP addresses constitute data.

‘Sensitive data’ are defined as details regarding a person’s personality, private affairs, state of health, economic situation, opinions and faith (ie, information included within the definition of ‘data’ other than personal

status and professional qualifications). In addition, 'sensitive data' include other information deemed to be sensitive data by order of the Minister of Justice with approval from the Constitution, Law and Justice Committee of the Knesset (no such order has been issued to date).

The Data Possession Regulations create an additional category of information called 'restricted data', which includes data about a person's health; data subject to the provisions of sections 13(e) of the Privacy Law (ie, primarily databases related to security, defence foreign affairs, law enforcement, taxation, and money laundering); and any other data deemed 'restricted' by an order of the Minister of Justice (no such order has been issued to date).

'Database' is defined as *'a collection of data, stored by magnetic or optical means and intended for computer processing'*, other than the following two specific kinds of databases: (i) any collection of data for personal use that are not used for business purposes; and (ii) a collection of data that contains only names, addresses and means of communicating with the data subject (eg, telephone, email address or fax numbers) which in itself does not create any characterisation that infringes the privacy of the people whose names are included in it, so long as neither the owner of the collection nor any body corporate under the owner's control has an additional collection of data (albeit unrelated to the first collection).

Collections of data that cannot be manipulated in a computerised manner (for example, collections of paper records, but not scanned versions of such records) are not included within the definition of 'database.' For this reason Directive 95/46/EC of the European Parliament, pursuant to which the European Commission formally adopted a decision recognising that Israel's domestic law guarantees an adequate level of protection for personal information for the purposes of Article 25 of the EU Data Protection Directive 95/46/EC applies only to international automated data transfers, as well as non-automated transfers that are subject to further automated processing in Israel, but not to international data transfers where the transfer itself, as well as the subsequent data processing, is carried out exclusively through non-automated means.

1.3.3 Types of acts/operations

The Privacy Law expressly addresses the following activities in respect of databases:

- managing a database;
- holding a database;
- using a database.

'Use' is defined as including, but not being limited to disclosure, transfer and delivery. While the Privacy Law does not specifically address or define the 'processing' of data, it can be presumed that processing activities are included within the definition of 'use'.

1.3.4 Exceptions

As described above, the following collections of data are not considered 'databases' under the Privacy Law: (i) collections of data that cannot be

manipulated in a computerised manner (ie, collections composed exclusively of paper records not in digital form); (ii) any collection of data for personal use that is not used for business purposes; and (iii) a collection of data that contains only names, addresses and means of communicating with the data subject (eg telephone, email address or fax numbers) which in itself does not create any characterisation that infringes the privacy of the people whose names are included in it, so long as neither the owner of the collection nor any body corporate under the owner's control has an additional collection of data. In addition, collections of data that do not relate to a 'person' as defined in the Privacy Law are not considered 'databases' under the Privacy Law and are not subject to the law's database provisions.

1.3.5 Geographical scope of application

Generally, the jurisdictional application of Israeli laws is limited to acts within Israel, although exceptions to this rule can be carved out in primary legislation or by case law. However, if the restrictions on the transfer of data (see section 8 below) are breached, any subsequent use of the data outside Israel is likely to be attributed to the party in Israel who breached the transfer restrictions.

1.4 Particularities

It should be noted that in January 2011, pursuant to the EU Data Protection Directive 95/46/EC, the European Commission formally adopted a decision that Israel's domestic law guarantees an adequate level of protection for personal information for the purposes of Article 25 of Directive 95/46/EC. This places Israel within the select number of jurisdictions so recognised by the European Commission. The decision applies to international automated data transfers, as well as non-automated transfers that are subject to further automated processing in Israel, but not international data transfers where the transfer itself, as well as the subsequent data processing, is carried out exclusively through non-automated means.

2. DATA PROTECTION AUTHORITY

In 2006, the Israeli Law Information and Technology Authority (ILITA) was established. ILITA sits within the Israeli Ministry of Justice, its head serves as the Registrar, and the ILITA staff implements the Registrar's functions. Technically, ILITA is comprised of the three statutory law and technology regulators set up under the Privacy Law, the Electronic Signature Act 2001 and the Credit Reporting Act 2002. Within ILITA, there are departments responsible for legal matters, enforcement and investigation, and registration and supervision. ILITA represents Israel in the international privacy arena and participates in the legislative process. Prior to the formation of ILITA, the Registrar served as Israel's data protection authority.

2.1 Role and tasks

The Registrar supervises the registration of databases, maintains the Registry of Databases, and supervises compliance with the Privacy Law and the regulations issued under it.

2.2 Powers

The Registrar is responsible for the registration and supervision of databases and is also the head of a unit set up by the Minister of Justice to supervise databases, their registration and the security of database information. The Registrar is authorised to appoint inspectors who are granted broad powers under the Privacy Law, including the right to demand that a person furnish information and documents related to a database. To ensure implementation of the Privacy Law and to prevent breaches, an inspector may enter any place in which he has a reasonable suspicion that a database is being operated, and search and seize any item (including computer equipment and output) if he is persuaded that doing so is necessary for the enforcement of the Privacy Law.

2.3 Priorities

The Registrar increasingly makes use of its supervisory and investigatory powers, including by performing investigations of businesses suspected of not complying with Privacy Law obligations. It is presumed that many of these efforts are aimed at preserving the confidence of EU countries following Israel's recognition by the European Commission as having an adequate level of protection for personal information. Indeed, many of the guidelines issued recently by the Registrar refer to terms and principles that appear in European legislation but do not appear in the Privacy Law (for example, certain of these guidelines call for data breach notifications and risk assessments, though these are not expressly required under the Privacy Law).

3. LEGAL BASIS FOR DATA PROCESSING

The Privacy Law does not expressly address the processing of personal data. However, as mentioned above, 'use' is defined as including, but not limited to, disclosure, transfer and delivery, and it can be presumed that processing activities are included within the definition of 'use'.

3.1 Consent

Consent is not necessarily required for the processing of personal data in a database so long as the information is used for the purpose for which it was provided. However, where data are collated without the consent of the data subject, the resulting database must be registered.

3.1.1 Definition

'Consent' is defined under the Privacy Law as informed consent, express or implied. While Israeli courts have not yet defined what constitutes informed consent for the purposes of the Privacy Law, in other contexts courts have interpreted 'informed consent' as consent granted after provision of information to an individual, which would be understood by a reasonable person, that is reasonably necessary for the purposes of providing consent.

3.1.2 Form

Consent may be express or implied. In many contexts, such as employment and health, it is standard practice to obtain written consents for the use,

processing and transfer of personal information.

3.1.3 In an employment relationship

Courts scrutinise consent very closely in employment contexts so that any suggestion, or even the subjective suspicion, of detrimental changes to the employee's conditions of employment can be deemed to be duress and so undermine the consent. In addition, any information gathered must be used for legal purposes, essential interests or a legitimate purpose and meet the proportionality test. As a matter of good practice, employment agreements governed by Israeli law should include the employee's express consent to the collation of personal data, including sensitive data, to the transfer of such data outside Israel and to the use of data for human resources management purposes.

3.2 Other legal grounds for data processing

In most situations, data processing will involve use of a database (as defined under the Privacy Law), and thus the notice requirement applicable to solicitations of information for inclusion in a database will apply (see section 4 below). There is no provision similar to Article 7 of the EU Data Protection Directive, but data must only be used and processed for the purpose for which they were provided.

3.3 Direct marketing and cookies

The Privacy Law regulates the operation and holding of databases used for direct mail services. 'Direct mail' is defined as *'an individual approach to persons, based on their belonging to a population group, as determined by one or more characteristics of those persons whose names are included in the database'*. An 'approach' includes one made in writing or in print, whether made via telephone, facsimile, computer or other means. 'Direct mail services' are defined as *'the provision of direct mail services to others by way of transferring lists, adhesive labels or data by any means whatsoever'*.

The Privacy Law prohibits a person from managing or possessing a database that is used for direct mail services unless it is registered and one of its stated purposes is direct mail services. A person who manages or possesses a database used for direct mail services must keep a record stating the source of the data, the date the data were received and the persons to whom the data were given.

Approaches by direct mail must state clearly: (i) that it is a direct mail solicitation; (ii) the registration number of the database; (iii) that the recipient of the solicitation has the right to be deleted from the database and the address to be contacted for this purpose; (iv) the identity and address of the database containing the data from which the solicitation was made; and (v) the sources from which the owner of the database received that data.

Every person has the right to demand that the owner of a database used for direct mail delete from the database any information relating to him or that personal information not be given to a specific person, to a category of persons, or to any person at all, whether for a specific or indefinite period of

time. The owner of the database must comply with these requests and give written notice of the fact that he has complied. If such notice is not given to the person within 30 days after the owner receives the request, then the person may apply to the Magistrates' Court for an order that the owner of the database comply with the request.

In December 2008, Israel enacted Amendment No. 40 to the Israeli Communications Law (Bezeq and Broadcasting) (Communications Amendment). The Communications Amendment prohibits the distribution of 'promotional messages' (defined below) by email, fax, automated calling system or electronic messages (SMS) without the recipient's opt-in (ie, obtaining the recipient's prior express consent), and its provisions are in addition to the Privacy Law provisions applicable to direct mail activities. The Communications Amendment defines 'promotional messages' as any commercial message which encourages the purchase of a product, service or other expenditure. The Communications Amendment applies equally to entities offering the goods or services themselves, and entities distributing electronic advertisements on their behalf. Consent may be obtained in writing, by electronic message or recorded conversation. Advertisers may contact business recipients once in order to solicit such consent; such initial contact will not be considered a violation of the Communications Amendment. Recipients may revoke their consent at any time, either in writing or in the same medium used to transmit the advertisement. It is permitted to distribute promotional messages without prior consent of the recipient under limited circumstances.

In addition to the consent requirements described above, the Communications Amendment requires that all electronic promotional messages include a clear, conspicuous notice containing the following information:

- identification of the promotional message as an advertisement. For email communications, the word 'advertisement' must appear in the email subject line; in all other promotional messages, such identification must appear in the beginning of the promotional message;
- the advertiser's identity and contact information; and
- notification of the recipient's right to opt out of receiving promotional messages and means for opting out (including an email address for email advertisements).

Israel does not have specific legislation directed to the use of cookies. Thus, the general privacy and data protection principles discussed elsewhere in this chapter will apply to the collection of information using cookies and use of such information.

3.4 Data quality requirements

Owners, holders and managers of databases are each responsible for data security, and 'data security' is defined to include, *inter alia*, the 'integrity of data' – ie, that the information in the database is identical '*to the source from which it was derived, without having been changed, delivered or destroyed without due permission*'. See also question 9.2 below.

3.5 Outsourcing

Outsourcing activities generally implicate the Privacy Law provisions applicable to databases, 'database holders' (since service providers will often qualify as database holders) and cross-border transfers of database information.

In 2011, ILITA published Directive 2-2011 for outsourcing activities. Under the directive (the legal status of which is not clear but which indicates the Registrar's interpretation of applicable law):

- service providers should preferably be given access to databases maintained and controlled by the database owner rather than receiving copies of databases;
- there should be an intercompany agreement expressly designating the scope and term of permitted access to and use of databases, ensuring the service provider's compliance with applicable laws (including notification requirements by the data subject, his rights to examine and correct the data, the need to separate different databases from different sources) and deletion of information following termination of the service period (unless keeping a copy is required by law or for the purposes of protection from lawsuit);
- it is recommended that a data security officer be appointed at both the client and service provider's facilities;
- entities outsourcing activities should create a binding data security policy; and
- the party outsourcing work should perform periodic service provider audits (and, when appropriate, surprise audits) to ensure compliance with obligations, and implementation of procedures for the service provider's transmission of breach notifications.

The guidelines do not limit other obligations existing under law.

3.6 Email, internet and video monitoring

3.6.1 General rules

Monitoring activities are highly regulated in the employment arena (see discussion below). Other monitoring activities will be subject to the general principles set forth in the Privacy Law and case law, including, without limitation, the prohibitions on violating personal privacy without consent and provisions applicable to databases (including, without limitation, the requirement that information in registered databases be used only for the purposes for which the database was registered, as well as the notice requirements for solicitations of database information (see section 4 below)).

With respect to email monitoring, copying or use of the content of an electronic message or other written communications not intended for publication without permission of the sender or intended recipient constitutes a breach of privacy unless the communication is of historic value or 15 years have passed since the day of writing; therefore, most email monitoring activities will require data subjects' consent.

In 2010 ILITA issued an opinion addressing video monitoring in public places. While the opinion primarily addresses video monitoring by public authorities, due to the practical difficulties involved in obtaining data

subject consent to video monitoring, the opinion and its recommendations are also directed at private entities performing monitoring activities in public places (under Israeli law, 'public places' are not limited to areas owned or managed by public authorities). While the opinion does not have the status of binding law, it demonstrates what the Registrar views as appropriate measures to be taken in relation to video monitoring.

Pursuant to the opinion, the following requirements are prerequisites to video monitoring activities in public places:

- performance of a privacy impact assessment addressing the specific purpose of video monitoring, the matters described below and evaluation of whether viable, less invasive alternatives exist;
- identification of a specific legitimate purpose for video monitoring, and results of monitoring may not be used beyond the specific legitimate purpose;
- video monitoring must meet the proportionality test, whereby it can be demonstrated that video monitoring is the most efficient and appropriate means for achieving the desired purpose, that such purpose cannot be achieved by less invasive means, and that the benefits will exceed the attendant invasion of privacy rights;
- the video monitoring must be implemented in a manner that causes least invasion of privacy (where cameras are situated, times during which they are activated, resolution, etc); and
- the public must be notified of video monitoring activities (for example, using appropriate signage).

If the results of video monitoring are maintained in database form, the database laws and regulations will apply. If the video monitoring will have voice recording capabilities, other requirements (such as the Eavesdropping Law 1979) will apply.

3.6.2 Employment relationship

Israel's highest labour court recently issued a decision which establishes for the first time comprehensive rules regarding employers' monitoring of employees' computer, information technology and email use at the their workplace. This decision stipulates that monitoring personal email correspondence requires a court order or employee consent in each instance; thus, in the wake of this decision, on a practical level it is difficult for employers to monitor employee communications unless the company IT policy prohibits employees' use of email for non-business purposes.

Pursuant to the labour court ruling the following are prerequisites for monitoring employees' computer, information technology and email use:

- Legitimate purpose. Monitoring must be in the interest of a legitimate business purpose. Data collected by virtue of monitoring activities may not be used in a manner different from the pre-defined legitimate purpose. The employer must examine alternative surveillance technologies which involve the lowest degree of violation of employee privacy.
- IT policy. The employer must implement a policy regarding computer

usage at the workplace and surveillance activities. This policy must be incorporated in the employment agreement.

- Detailed notice. The IT policy must provide specific and detailed notice regarding monitoring activities to be undertaken which includes: express notice that email communications will be monitored and for what purpose; description of monitoring and surveillance measures and technologies which will be used (identifying specific programs); identification of frequency of monitoring activities and which communications will be monitored; the manner in which the gathered data will be kept and stored; the duration of such storage; and what use, if any, will be made of the stored data. To the extent the employer intends to employ blocking technologies (for example, blocking transmission of emails containing certain types of data or access to certain websites) the employer must clearly detail the scope of such technologies and their use.
- Written consent. The employee must consent in writing to the violation of his privacy (certain mandatory language is required to appear in the consent) and this consent must be part of the employment contract. The consent must be explicit, informed and voluntary, after the employee has been notified of the employer's intention to violate the employee's privacy interests.
- Third party notice. Third parties must be notified of surveillance activities (for example, by means of an email footer containing appropriate disclosure).

As this decision was only recently enacted, the requirements for implementing certain of these requirements remain somewhat unclear and have not yet been clarified by subsequent court decisions. Many Israeli companies are currently engaged in efforts to comply with the ruling.

4. INFORMATION OBLIGATIONS

Any solicitation of information for inclusion in a database or use as part of a database must be accompanied by a notice to the data subject.

4.1 Who

Any person or entity soliciting information for inclusion in a database.

4.2 What

The notice must indicate: (i) whether the person has a legal obligation to deliver the requested data or whether delivery is voluntary; (ii) the purpose for which the data are requested; and (iii) to whom data will be delivered and for what purpose.

4.3 Exceptions

The notice requirement applies to information included in a database. Thus it does not apply to solicitations of data to be stored in a form that will not constitute a 'database' as defined under the Privacy Law.

4.4 How

No specific form of notice is required.

5. RIGHTS OF INDIVIDUALS

5.1 Access

5.1.1 Right

The Privacy Law provides that an individual may inspect any information about the individual that is kept in a database, whether in person, by a representative who has written authorisation, or by a guardian (eg in the case of minors). The owner of the database must enable inspection of the information in Hebrew, Arabic or English, as requested. Where a database is maintained by a third party (ie, the database holder), the database owner must refer the applicant to the holder and provide the holder's address. Also, the database owner must give written instructions to the holder to permit the inspection. If the applicant applied first to the database holder, then the holder must inform the applicant whether he holds information about the applicant and provide the database owner's name and address.

The Data Inspection Regulations permit (but do not require) the database owner to provide a print-out of the requested information in lieu of permitting inspection of the data within the database. The person viewing the print-out may not remove the print-out from the premises of the database owner or holder without permission.

5.1.2 Exceptions

The right of access does not apply where:

- the data concern the applicant's physical or mental health and the database owner believes that the data may endanger the applicant's life or cause severe harm to the applicant's physical or mental health (in such cases, the database owner must deliver the data to a physician or psychologist on behalf of the applicant); or
- the data are privileged (for example, information held by attorneys, physicians, psychologists, or social workers) and access constitutes a violation of the privilege pursuant to statutory or judicial law, unless the applicant is the person for whose benefit the privilege is enacted.

In addition, the right of inspection does not apply to the following databases and data:

- a database of a security authority (ie, the police, the intelligence branch of the General Staff, the military police of the Israel Defence Forces, the General Security Service, the Institute of Intelligence and Special Assignments, and the Witness Protection Authority);
- the prison service database;
- a tax authority's database;
- data to which the security of the state, its foreign relations or the provisions of any enactment require that they not be disclosed;
- databases of any body deemed (by the Minister of Justice, in consultation with the Minister of Foreign Affairs or Defence, with approval of the Parliament Foreign Relations and Security Committee) to contain information that should not be revealed due to national security or foreign relations ('secret information'). Databases deemed to contain secret information include the databases of the Ministry

of Defence and certain of its affiliates, and the Israel Aircraft Industry and its subsidiaries and operating units. However, any person who asks to inspect data about himself stored in such a database is entitled to examine any information that is not 'secret information';

- databases of investigations and law enforcement, including those maintained by the Police Investigation Department in the Ministry of Justice (in matters of investigations and enforcement), the Israel Securities Authority (in matters of investigations), and the Israel Antitrust Authority (in matters of investigations); and
- the database established by the Minister of Justice in accordance with section 28 of the Prohibition of Money Laundering Law 2000, which contains a record of all reports of money laundering submitted to the Ministry of Justice. This database is governed by the Prohibition on Money Laundering Regulations (Guidelines for Management of the Database and the Protection of Data contained in it), 2002.

A database holder may refuse the request for inspection if the database is held by a 'service bureau' that processes and stores data for its customers, so long as the applicant is referred to the owner of the data on whose behalf the processing or storage services are performed. If the owner of the database refuses to permit inspection, the applicant must be notified within 21 days (which may be extended by the Registrar for 15 additional days).

5.1.3 Deadline

Inspection must be permitted within 30 days of the data subject's request, although the Registrar may extend the period by an additional 15 days.

5.1.4 Charges

The owner or holder of the database is entitled to impose a fee of NIS 20 for the inspection.

5.2 Rectification

5.2.1 Right

If an individual's inspection reveals that database information is inaccurate, incomplete, unclear or not up to date, the individual may request that the database owner (or, if the owner is a foreign resident, the database holder) amend or delete the information. If the database owner agrees to the request, he must make the necessary changes and communicate them to the applicant and to anyone who received the information from him within the preceding three years.

5.2.2 Exceptions

No exceptions are foreseen.

5.2.3 Deadline

If the database owner refuses the request for correction, then he must give the person notice of the refusal within 30 days of receipt of the request (which may be extended for an additional 15 days by the Registrar). The holder of the database must correct the data if the database owner agreed to

the requested amendment, or if a court ordered the correction to be made.

5.2.4 Charges

The issue of charging is not addressed.

5.3 Erasure

5.3.1 Right

There are no provisions in the Privacy Law or regulations regarding erasure of data in databases generally. However, a person may demand in writing that the owner of a database used for direct mail delete the information about him from the database. In addition, recent non-binding communications originating from the Registrar derived from the Privacy Law provide an obligation to remove database information when its intended purpose has expired.

5.3.2 Exceptions

Not applicable.

5.3.3 Deadline

Not applicable.

5.3.4 Charges

Not applicable.

5.4 Blocking

5.4.1 Right

The Privacy Law and regulations do not include provisions regarding blocking of data in databases generally. However, every person may demand in writing from the owner of a database used for direct mail, or from the owner of a database containing data on the basis of which the direct mail approach was made, that data relating to him not be given to a specific person, to a category of persons, or to any person at all, either for a specific or indefinite period of time.

5.4.2 Exceptions

Not applicable.

5.4.3 Deadline

Not applicable.

5.4.4 Charges

Not applicable.

5.5 Objection

Since the Privacy Law does not specifically address processing of data, the law does not create a general right to object to such processing. However, the Privacy Law allows a data subject to object to processing of data by means of a civil suit based on the claim that the processing is an infringement of privacy or constitutes an act or omission in violation of Chapters Two or

Four of the Privacy Law. A limited right of objection exists with respect to direct mail services (see section 3.3 above).

5.5.1 Right

Not applicable.

5.5.2 Exceptions

Not applicable.

5.5.3 Deadline

Not applicable.

5.5.4 Charges

Not applicable.

5.6 Automated individual decisions

5.6.1 Right

The Privacy Law does not create any such right.

5.6.2 Exceptions

Not applicable.

5.6.3 Deadline

Not applicable.

5.6.4 Charges

Not applicable.

5.7 Other rights

Not applicable.

5.7.1 Right

Not applicable.

5.7.2 Exceptions

Not applicable.

5.7.3 Deadline

Not applicable.

5.7.4 Charges

Not applicable.

6. REGISTRATION OBLIGATIONS

Database owners are required to register certain databases with the Database Registrar.

The Privacy Law and regulations do not impose obligations to notify the

Registrar of data processing operations or data transfers.

6.1 Notification requirements

6.1.1 Who

Database registration requirements apply to the database owner. However, the Privacy Law prohibits managing or holding a database that is required to be registered but has not been registered; thus database managers or database holders could also face liability in connection with a database that is not registered in the manner required under law.

6.1.2 What

The owner of a database must register the database if any of the following conditions is met:

- the database contains data about more than 10,000 people;
- the database contains sensitive data;
- the database contains data about natural persons not provided by them, on their behalf or with their consent;
- the database belongs to a public body (as defined under section 23 of the Privacy Law; or
- the database is used for direct mail.

In addition, the Registrar has the power to order that databases which are exempt from the obligation to register pursuant to the exception above must nonetheless be registered. The Registrar has not yet used this power.

6.1.3 Exceptions

Even where one of the conditions above are met, the database registration requirements do not apply where the database only contains information made public by lawful authority, or which was made available for public inspection by a lawful authority. This exemption recognises that under Israeli law, certain databases must be open to public inspection, such as the database containing information about companies pursuant to the Companies Law 1999. The Registrar has the power to order that databases that are exempt from the obligation to register pursuant to the exception above must nonetheless be registered. The Registrar has not yet used this power.

6.1.4 When

A database must be registered prior to managing or holding the database, unless the Registrar permits performing such acts prior to registration.

6.1.5 How

Applications to register a database must be submitted to the Registrar using the application form published by the Registrar and available (in Hebrew) on the ILITA website, www.justice.gov.il/NR/rdonlyres/1E830B68-FC40-4B60-A154-45BA9C144863/12412/tofesrishummaagar.pdf. The application must specify the following:

- the identity and address in Israel of the owner of the database, the database holder and the manager of the database;

- the purpose for setting up the database and the purposes for which the information is intended;
- the types of data to be included in the database;
- details regarding transfers of data outside the borders of the state; and
- details regarding any regular receipt of data from a public body, the name of the public body providing the data and the nature of the data, with the exception of details delivered by the public body with the consent of the data subjects.

In addition, the general manager of the database owner must notify the Registrar in writing of the name of the database manager for inclusion in the Registry.

The owner or holder of a database must notify the Registrar if there is a change in the details provided in the application, or if operation of the database is discontinued. If the Registrar deems it appropriate with respect to the actual operations of the database, the Registrar is authorised to register a purpose different from that specified in the application, to register a number of purposes for a database, or to order that several applications be submitted instead of the single application that was submitted.

Following submission of the application for registration of a database, the Registrar must register it in the register within 90 days, unless the Registrar has reasonable grounds to assume that the database is used or is liable to be used for illegal activities or as a cover for illegal activities or the data included in the database were obtained, accrued or collected in violation of the Privacy Law or in violation of the provisions of any other legislative enactment. If the Registrar does not register the database within 90 days and does not inform the applicant that registration has been refused or delayed, then the applicant is permitted to manage or hold the database even if it is not registered. However, if the Registrar does inform the applicant of a refusal or delay in registration, then the applicant may not manage or hold the database unless a court decides otherwise.

6.1.6 Notification fees

Pursuant to the Privacy Regulations (Fees) 2000, as amended in December 2010 and January 2011, the initial fee for database registration is NIS 251. An additional annual fee is imposed on registered databases for subsequent calendar years, with the exception of databases owned by the State of Israel. The amount of the fee is determined taking into account the owner of the database and its contents. The fee for the registration of a database owned by a corporation, other than a non-profit organisation, is NIS 939 if the database contains sensitive data concerning more than 10,000 people; NIS 501 for sensitive data concerning 10,000 people or less; and NIS 251 for any other database. Registered databases not owned by a corporation, or owned by a non-profit organisation, are exempt from payment, unless the database contains sensitive data concerning more than 500 people, in which case the fee is NIS 250. Special discounts are granted to owners of multiple databases.

6.2 Authorisation requirements

Not applicable.

6.2.1 Who

Not applicable.

6.2.2 What

Not applicable.

6.2.3 Exceptions

Not applicable.

6.2.4 When

Not applicable.

6.2.5 How

Not applicable.

6.2.6 Authorisation fees

Not applicable.

6.3 Other registration requirements

6.3.1 Who

Not applicable.

6.3.2 What

Not applicable.

6.3.3 Exceptions

Not applicable.

6.3.4 When

Not applicable.

6.3.5 How

Not applicable.

6.3.6 Registration fees

Not applicable.

6.4 Register

The Registrar is required to maintain a Registry of Databases. All of the details required to be included in the application for registration must be included in the Registry. The Registry is open for public inspection (with the exception of certain governmental databases such as the police and those maintained by the military and tax authorities).

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

The following entities must appoint a suitably trained person to be in charge

of data security ('the Security Officer'):

- entities holding five or more databases requiring registration;
- public bodies, as defined in section 23 of the Privacy Law; and
- banks, insurance companies or companies involved in ranking or evaluating credit.

The database manager must inform the Registrar as to the identity of the Security Officer.

7.2 Tasks and powers

While the Security Officer is to be responsible for data security, the database owner, holder and manager nevertheless are each held individually responsible under the Privacy Law for data security as well.

8. INTERNATIONAL DATA TRANSFERS

8.1 Applicable rules

Under the Data Transfer Regulations, the transfer of data from databases within Israel to a location outside the State of Israel is strictly prohibited unless the database owner secures the written undertaking of the recipient of the transferred data that such recipient will take sufficient precautions to protect the privacy of the data subjects and will not transfer the data to anyone else. In addition, an international transfer may not be made unless one (or more) of the criteria set forth below are met.

8.2 Legal basis for international data transfers

Pursuant to the Data Transfer Regulations, the following constitute the legal basis for international transfers of data:

- the data are transferred to a country the laws of which ensure that the transferred data are protected to a degree no less than that accorded by Israeli law and incorporate the following principles: (i) data must be gathered and processed legally and fairly; (ii) data shall be held, used and transferred solely for the purpose for which they were received; (iii) stored data shall be correct and current; (iv) data subjects shall have the right to view and correct the data; and (v) proper security precautions should be implemented to protect the data;
- the data subject has consented to the transfer;
- the transfer is critical to the subject's health and he or she is unable to give consent;
- the data are transferred to a corporation in which the owner of the Israeli-based database has a controlling interest (ie over 50 per cent) and the corporation has undertaken to maintain the privacy of the data;
- the recipient undertakes toward the owner of the Israeli-based database to uphold the laws regarding the holding and using of data applying to databases located in Israel;
- the data have been lawfully publicised;
- transfer of data is necessary for the benefit or the security of the public;
- transfer of data is required under Israeli law; or
- data are transferred to a database in a country: (i) which is a party to the

Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (the Convention); (ii) which receives data from other European Union member countries under the same terms and conditions (which has been interpreted by the Registrar to include entities participating in the US Safe Harbour scheme) ; and/or (iii) which, according to a declaration issued by the Israeli Registrar, has a privacy protection authority with which the Registrar has reached a co-operative understanding.

8.2.1 Legal basis for international agreements.

As mentioned above, under the Data Transfer Regulations, the transfer of data outside the State of Israel is strictly prohibited unless the database owner secures the written undertaking of the recipient of the transferred data that such recipient will take sufficient precautions to protect the privacy of the data subjects and will not transfer the data to anyone else. In addition, as described above, a transferee undertaking toward the owner of the Israeli-based database to uphold the laws regarding the holding and using of data applying to databases located in Israel can also serve as legal basis for the international transfer of data. The European Commission's standard contractual clauses can be used where they are revised to incorporate the mandatory Israeli provisions described above.

8.2.2 Binding corporate rules

Not applicable.

8.2.3 Safe Harbour

Not applicable.

9. SECURITY OF DATA PROCESSING

9.1 Confidentiality

Personal information contained in databases is considered confidential, and a person may be subjected to five years' imprisonment for disclosing data obtained by virtue of his or her position as an employee, manager or holder in respect of a database, except for the purpose of performing his or her duties or implementing the Privacy Law or under a court order in connection with legal proceedings.

9.2 Security

The Privacy Law contains specific provisions regarding the security of data in databases. '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'*. The phrase 'integrity of data' is defined to mean that the information in the database is identical *'to the source from which it was derived, without having been changed, delivered or destroyed without due permission'*. Owners, holders and managers of databases are each responsible for data security.

Pursuant to the Data Possession Regulation, maintaining database security

includes: (i) ensuring physical protection of the automatic data processing system and infrastructure; (ii) setting administrative procedures regarding permitted access to the data and instructions regarding their collection, verification, processing and distribution (such procedures are also applicable to anyone providing external services to the database owner); (iii) granting access authorisation to the database and restricting the access of authorised users in accordance with the instructions of the Data Transfer Committee (a committee to be appointed by each public body); (iv) preparation of an updated list of authorised users according to the various degrees of authorisation; (v) ensuring the authorised users sign undertakings to maintain the confidentiality of the data and to uphold the Data Transfer Committee instructions; (vi) establishing operating procedures for the system, including data security and protection for the integrity of data; (vii) implementing reasonable security measures, in accordance with the level of sensitivity of the data, that will prevent intentional or accidental access to the system by a user beyond the areas of data permitted to him; and (viii) establishing controls to reveal damage to the integrity of the data and repair defects.

Additional requirements apply in respect of 'restricted data' and include the following: (i) the database must be administered according to guidelines for security and supervision of physical storage of the data (including a chapter governing any external service provider performing services such as data entry, data processing, etc); (ii) any print-outs containing restricted information that are distributed by a public body must state on each page that the information contains data protected by law and that unauthorised distribution is a crime; (iii) the database manager must maintain a list of the users of the restricted information, and a list of those permitted access to the data (including their identification numbers, access codes and the type of information to which they are permitted access); the access codes must be changed periodically and not less than once every six months or upon a change of employees; (iv) restrictions on access to the back-up copies of restricted information; (v) documents and magnetic records of intermediate processing activities must be burned, shredded or otherwise destroyed; and (vi) the database manager must keep a journal of atypical events and save it for three years.

Under Directive 1-2010 published by the Registrar, where data subjects can remotely access personal data stored in a database, the database owner must implement a verification process that requires the data subject to submit at least one item of data which should only be known to the data subject. The number of verification items required should rise in accordance with the sensitivity of the data, or alternatively, other measures could be employed, such as identity verification by means of a SIM card, cellular phone or biometric characteristic. Failure to correctly assess the sensitivity of the data and adjust the requirements accordingly constitutes a breach of data security obligations.

The Privacy Protection Council (an entity established by the Minister of Justice to advise on matters related to the Privacy Law and to provide guidance to the Registrar and the Israel Chamber of System Analysts (a

nonprofit IT and information systems professional organisation) have issued a set of (non-binding) guidelines intended to assist database managers in implementing the Privacy Law - they can be accessed at: www.justice.gov.il/NR/rdonlyres/C0681561-6CD4-4A6E-AE85-E2ABACC2C171/0/parta.pdf.

9.3 Data security breach notification

Data security breach notification is not required under the current law; however, if the draft Protection of Privacy Regulations (Information Security in Databases) 2010 are enacted as law, they will require the data security officer to document events of a possible breach of the database (if possible, by automatic documentation), and the security policy of a medium to high security database would have to include provisions for the report to the database owner of security breaches. ILITA's Directive 2-2011 on outsourcing requires service providers to provide immediate breach notifications of possible security failures to the database owner (see section 3.5 above).

9.4 Data protection impact assessments and audits.

Such assessments and audits are recommended in certain circumstances pursuant to the Directive and the non-binding guidelines published by the Registrar (see sections 3.5, 3.6.1 and 3.6.2 above).

10. ENFORCEMENT, SANCTION, REMEDIES AND LIABILITY

10.1 Enforcement action

The Registrar has the authority to suspend or rescind database registrations due to a failure to comply with database laws. The Registrar has also issued notices of non-compliance.

10.2 Sanction

The Registrar may impose the following administrative fines:

- using, holding or managing an unregistered database requiring registration in breach: NIS 2,000;
- use of database information for purposes differing from those for which the database was registered: NIS 5,000;
- delivering false information in a database registration application: NIS 2,000;
- failing to deliver information or delivering false information in a notice soliciting information for inclusion in a database: NIS 3,000;
- failing to comply with data subjects' inspection rights: NIS 3,000;
- granting access to a database to someone not authorised under the written agreement between data subject and database owner: NIS 3,000;
- failing to deliver documents or an affidavit to the Registrar where required by a holder of at least five databases: NIS 2,000;
- failing to appoint a security officer for data security for databases which are so required by law: NIS 3,000;
- managing or possessing a database used for direct mail services without designation such use in the database registration: NIS 3,000;
- managing or possessing a database used for direct mail services 17E

- without properly tracking of sources of information used: NIS 2,000;
- managing or possessing a database used for direct mail services without properly notifying database subjects or responding to requests for removal: NIS 3,000.

Pursuant to the Administrative Offence Regulations (Administrative Fine – Protection of Privacy) 2004, a five-fold fine for every type of violation can be imposed upon a corporation. For continuing violations, one-tenth of the fine can be imposed for each day of violation after service of warning of the breach. As mentioned above, draft legislation, if enacted, would substantially increase fines which the Registrar is entitled to impose.

10.3 Examples of recent enforcements of data protection rules

In recent years, ILITA has issued administrative fines for database violations, issued notices of non-compliance and de-registered databases and ordered the destruction of database contents. Situations in which administrative fines have been imposed include:

- failure to include full details in a notice for solicitation of database information;
- violation of direct mail provisions of the Privacy Law;
- illegal trading in databases;
- use of an illegal online database for marketing purposes;
- use of database information for purposes other than those for which the database (a voter registry) was established and delivering of false details in a registration application;
- use of information provided by a customer in order to solicit him for other purposes.

The amount of fines imposed ranged from several thousand NIS to NIS 258,000.

10.4 Judicial remedies

An infringement of privacy is actionable as a civil wrong pursuant to Privacy Law, and a claimant may obtain monetary compensation or injunctive relief. Violations of Privacy Law sections 2(7), 2(9), 2(10) or 2(11) (ie, infringing an obligation of secrecy laid down by law in respect of a person's private affairs; using, or passing on to another, information on a person's private affairs other than for the purpose for which it was given, publishing or passing on anything that was obtained by way of an infringement of privacy under certain provisions of the Privacy Law or publishing any matter that relates to a person's intimate life, state of health or conduct in the private domain) are subject to five years' imprisonment. No civil or criminal action may be brought for violations with no real significance.

A court may award damages amounting to NIS 50,000 without proof of damages for breach of privacy rights, and damages may be doubled where the privacy infringement was with intent to harm.

10.5 Class actions

The Privacy Law does not expressly authorise class action claims for privacy

or database violations. However, the Class Action Law 2006 provides a closed list of circumstances under which class actions may be brought. For example, class actions may be brought against a vendor, supplier, manufacturer, importer or marketer of a product or service, with regard to the relationship between it and a customer, and a number of privacy and database-related class actions have been brought in Israeli courts under this provision. There are additional grounds for class actions which may be relevant to the data protection context as well (for example, class action claims are permitted under certain circumstances against a bank or insurer).

10.6 Liability

Violators may be subjected to five years' imprisonment for disclosing data obtained by virtue of his position as an employee, manager or holder in respect of a database, except for the purpose of performing his duties or implementing the Privacy Law or under a court order in connection with legal proceedings.

Violators may be subjected to one year's imprisonment for breach of the following obligations regarding databases: (i) managing, possessing or using a database in breach of Privacy Law (ie, the obligations to register certain databases); (ii) delivering false details in an application for registration of a database in violation of Privacy Law ; (iii) failing to deliver details or delivering false details in a notice attached to a request for information under Privacy Law section 11; (iv) failing to comply with the provisions of Privacy Law, regarding the right to inspect information kept in a database, or failing to amend a database in accordance with the requirements of Privacy Law ; (v) granting access to a database in breach of Privacy Law, or failing to deliver documents or an affidavit to the Registrar in accordance with the provisions of the Privacy Law; (vi) failing to appoint a security officer for data security as required by the Privacy Law; (vii) managing or possessing a database used for direct mail services in breach of the provisions of the Privacy Law regarding direct mail; and (viii) delivering information in breach of the Privacy Law (regarding public bodies).

These are strict liability offences, as neither criminal intent nor negligence need be proven.

There are no provisions specifically setting out rights to compensation for damage suffered as a result of inaccurate data. However, since breaches of the Privacy Law are actionable as civil torts, compensation for damage arising from use of inaccurate data maintained in violation of the Data Possession Regulations could theoretically be awarded.

In addition to providing that an infringement of privacy is actionable as a civil wrong, the Privacy Law also specifies that an act or omission in breach of the provisions of Chapter Two (protection of privacy in a database) or Chapter Four (delivery of information by public bodies), or in breach of any regulations issued pursuant to the Privacy Law, is a civil wrong under the Civil Wrongs Ordinance (new version). This provision was added in order to ensure that even omissions such as a failure to ensure data security would also be actionable as a civil wrong.