

# Israel

**Yigal Arnon & Co** Yoheved Novogroder-Shoshan\*

---

## 1. LEGISLATION

### 1.1 Name\title of the law

The Protection of Privacy Law 1981 (the '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 (the '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 (the '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 (the 'Data Transfer Regulations');
- Protection of Privacy Order (Determination of Public Bodies) 1986;
- Protection of Privacy Order (Determination of the Investigatory Authority) 1998; and
- 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 Inclusion of Biometric Identification Means and Data in Identifying Documents and Databases Law 2009 (establishing a biometric database); 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 in this chapter relate to the Privacy Law as supplemented by complementary regulations and case law.

## **1.2 Pending legislation**

Three major pieces of legislation are pending.

The draft Protection of Privacy Law (Reduction of Registration Requirements and Establishment of Obligation to Maintain Management Procedures, Work Processes and Documentation) 2012 represents a fundamental shift in the Israeli approach to database regulation. The proposed amendment would replace database registration requirements for most databases with accountability, internal documentation and notification requirements.

Database owners and holders will be required to implement internal management procedures and methodologies designed to meet Privacy Law requirements and to maintain appropriate, up-to-date documentation in respect of such efforts (including documentation with respect to database management, use and security and the exercise of persons' inspection and correction rights). In addition, database owners must maintain a document containing certain basic information regarding the database, and such document must be made available for public inspection upon request. Database owners must notify the General Director of Data Protection of the existence of the database and related information and that the documentation requirements have been complied with. Database registration requirements would continue to apply to a limited number of databases, primarily those generated for the purpose of trading in information (for example, databases used to provide direct mail services), databases maintained by private investigators or providers of credit-rating services and databases maintained by public bodies.

The aforementioned obligations would apply to databases which include the following categories of data: (i) data about a person's personal, private affairs, including data about his or her behaviour in the private domain; (ii) medical data; (iii) genetic data as defined in Genetic Information Law 2000; (iv) economic data; (v) data regarding a person's political opinions or religious beliefs; (vi) criminal background data; (vii) location data, subscription data or traffic data; and (viii) biometrics, which may be measured by computers and are used to identify individuals.

The draft Protection of Privacy Regulations (Information Security in Databases) 2012, 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.

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') (who would be renamed the 'General Director of Data Protection'), 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 General Director of Data Protection to exercise certain powers that are currently held only by the criminal enforcement authorities.

### 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.

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 sex life, state of health or conduct in the private domain.

Section 2 of the Privacy Law also prohibits spying on or tracking a person in a manner likely to harass him/her, 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.

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 suggests that in certain cases corporations may, to some extent, also 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, 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) 2012 compares the role of the database owner to that of the ‘data controller’ under the *EU Data Protection Directive 95/46/EC* (the ‘Directive’); 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/her 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’ is 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 persons’ addresses, telephone numbers, bank account information, national ID numbers, IP addresses and digitised images of the interior of one’s property constitute data.

‘Sensitive data’ is 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 includes 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, the Israeli Parliament (no such order has been issued to date). Under the draft Protection of Privacy Law (Reduction of Registration Requirements and Establishment of Obligation to Maintain Management Procedures, Work Processes and Documentation) 2012, this category would be deleted.

The Data Possession Regulations create an additional category of information called ‘restricted data’, which includes, in particular, data about a person’s health; 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', with the exception of three specific kinds of databases (see section 1.3.4 below).

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, the adequacy finding of the European Commission pursuant to Article 25 of the Directive regarding Israel only applies to international automated data transfers, as well as non-automated transfers that are subject to further automated processing in Israel, but not to 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; and
- 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 data processing activities are included within the definition of 'use'.

### **1.3.4 Exceptions**

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 person (eg telephone, email address or fax numbers) which in itself does not create any characterisation that infringes the privacy of the persons 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 any 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.

### **1.3.6 Particularities**

In January 2011, the European Commission formally adopted a decision that Israel's domestic law guarantees an adequate level of protection for personal data. This places Israel within the select number of jurisdictions so recognised by the European Commission. The decision applies to automated data transfers, as well as non-automated transfers that are subject to further automated data processing in Israel, but not 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 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.

*HaReshut LeMishpat, Technologia V'Meida* (Israeli Law Information and Technology Authority)

Ministry of Justice

PO Box 7360

The Government Offices

125 Begin Street

Tel Aviv

Israel 61072

T: +972 3 7634 050

F: +972 2 6467 064

W: <http://index.justice.gov.il/Units/ilita/Pages/default.aspx>

### **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/she has a reasonable suspicion that a database is being operated, and search and seize any item (including computer equipment and output) if he/she is persuaded that doing so is necessary for the enforcement of the Privacy Law.

### **2.3 Priorities**

In recent years, the Registrar has dramatically increased its supervisory, investigatory and enforcement activity, including by performing investigations of businesses suspected of not complying with Privacy Law obligations. .

## **3. LEGAL BASIS FOR DATA PROCESSING**

Data may be used for the purpose for which it was provided without the need for consent or another legal ground. The Privacy Law does not have specific requirements for the processing of sensitive or restricted data.

### **3.1 Consent**

The Privacy Law does not expressly require persons' consent for the processing of data in a database so long as the information is used for the purpose for which it was provided but consent legitimises the use of data for secondary purposes. Where data is collated without the consent of the person, the resulting database must be registered.

#### **3.1.1 Definition**

'Consent' is defined under the Privacy Law as informed consent – either 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 a person, which would be understood by a reasonable person and which is reasonably necessary for the purposes of providing consent.

#### **3.1.2 Form**

Consent may be either express or implied. In many contexts, such as employment and health, it is standard practice to obtain written consent for the use, processing and transfer of data.

For specific form requirements in relation to direct marketing, see section 4.9 below.

### **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 data for inclusion in a database will apply (see section 4 below). There is no provision similar to Article 7 of the Directive, which lists the legal grounds for the processing of data, but data must only be used and

processed for the purpose for which it was provided by the person.

### **3.3 Codes of conduct**

Not applicable.

## **4. SPECIAL RULES**

### **4.1 Employment**

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

With respect to limitations placed on monitoring employees' use of the Internet and on monitoring employees by means of video cameras, see section 4.8 below.

### **4.2 Health**

Health-related data falls within the definitions of both 'data' and 'sensitive data', and accordingly such data is subject to the Privacy Law requirements. Since health-related data is considered 'sensitive data', databases containing information about a person's health condition must be registered with ILITA.

In addition, medical data is deemed to be 'private affairs'. Consequently, breach of confidentiality obligations in relation to medical data may constitute an infringement of general privacy rights under the Privacy Law, and may subject the infringer to civil penalties, and to criminal penalties more stringent than those relating to the infringement of database-related requirements.

Furthermore, the regulations governing 'restricted data', which require additional security measures, apply to databases containing data about a person's condition of health.

As an exception to persons' data inspection rights, database owners are entitled to withhold physical or mental health-related information where the database owner believes the information could cause severe harm to the person or endanger his or her life. The information must, however, be provided to the person's physician or psychologist.

The Genetic Information Law 2000 specifically requires the holder of a database of identified genetic information to register it in accordance with the Privacy Law. Identified genetic information is defined as information derived from genetic tests, and accompanied by an identifying detail, defined as a person's name, identification number or any other identifying number issued by a governmental authority.



A number of other laws and directives impose on care-providers, employees and medical institutions an obligation of secrecy regarding patient information, such as the Patients' Rights Law 1996, the Treatment of the Mentally Ill Law 1991 and the Psychologists' Law 1977.

### 4.3 Finance

The collection and dissemination of credit data has been regulated in the Credit Details Service Law 2002 (the 'Credit Law'). This Law applies to both credit data services and business information services.

The Credit Law requires anyone engaged in providing these services to obtain a licence as a credit-reference agency and to register his/her database(s) in accordance with the Privacy Law. Under the Credit Law, the Minister of Justice has appointed a registrar for both credit data services and business information services. The registrar's duties include the issuance of licences to database owners and managers, the compilation of a register of licensed holders and the supervision of licence holders. A transferor of information to a licensed owner of a credit database in accordance with the law is not liable under the Privacy Law.

With regard to credit data, the Credit Law distinguishes between data regarding the person's non-payment of debts, and 'positive data', defined as data regarding credit that was issued to a consumer. A credit report must include both types of data, but while information regarding non-payment of debts may be obtained from a number of sources as specified in the law, 'positive data' may only be obtained from a banking corporation, unless the subject has consented to the collection and provision of such data in a written notice to the registrar or the licence holder. The registrar must keep a list of persons who have consented in this manner, and upon request in writing from the person, must delete him/her from the list. A partial credit report, containing data from only some of the sources listed in the law, may also be issued, provided that the report clearly states that the information is partial, in a manner to be determined by the Minister of Justice.

The law contains a number of provisions relating to the collection and dissemination of credit data. For example, credit data may only be retained for seven years, after which it must be destroyed. A credit report may only include the information detailed in the law, and may only be used for limited purposes. In order to receive a credit report, a person must provide a written statement explaining the purpose for which the information will be used. The person to whom the data relates is entitled to receive, free of charge and within seven days of request, a credit report relating to him-/herself, to inspect the relevant data, and may contact the licence holder if he/she believes that the data is not true, complete, clear or current. Violations of the law are subject to fines and, under certain circumstances, imprisonment.

In addition, the protections of the Privacy Law apply generally to the collection and disclosure of any information relating to an individual's financial position and credit history. Specific mention of credit data is contained in a provision on security in the Privacy Law, which requires that

companies engaged in ranking or evaluating credit ratings must appoint a suitably trained person to be in charge of data security.

Israeli banking laws do not include specific provisions regarding confidentiality of clients' information. However, the requirement to maintain such confidentiality has been established by case law in reliance on the Privacy Law, English law and banks' fiduciary duties. In one notable case, the Supreme Court addressed whether banks may in certain instances have a fiduciary duty to share client confidential information with other clients. In that case, the Court addressed the question whether the bank had a fiduciary duty to disclose information regarding a bank client, a construction company on the verge of bankruptcy, to an individual seeking a mortgage from the bank to purchase an apartment from the construction company. The Court held that in determining whether to disclose the information, the bank must consider the nature of the intended transaction between the two clients, the objective and subjective characteristics of the clients, the level of reliance of the client on the transaction and on the bank and the bank's interest (Civ. App. 5893/91 *Tefachot Israeli Mortgage Bank v Nathan Zabach Padi* 48 (2) 573). The Supreme Court has also established criteria for the disclosure of financial data in the context of lawsuits, which include: the level of indispensability of the information to the case; whether there are means which are less injurious to the client's confidentiality; and the need to limit the scope of disclosure as much as possible (Civ. App. 1917/92 *Yaakov Scholar v Nitza Jerby Padi* 47 (764)).

#### **4.4 Telecommunications**

Not applicable (but see section 4.9 below).

#### **4.5 Historical, statistical and scientific research purposes**

The Privacy Law prohibits the copying of 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. Thus, while the various general provisions of the Privacy Law and regulations with respect to databases would apply to the use of a collection of historical data and documents if stored by magnetic or optical means, there would be no prohibition per se to copy and use a letter or electronic message of historic value or of the required age, even without the consent of the sender or the recipient.

#### **4.6 Children**

In December 2010, the Registrar published draft ethical and behavioural guidelines for database owners collecting data from minors. ILITA has indicated that the draft guidelines are respected in practice, though it is not clear whether or when final guidelines will be issued. The proposed guidelines are aimed at forcing those who collect data from minors to act responsibly, and receive parental consent to use the data, while giving clear explanations as to how they intend to use the data, so that the parents

can exercise discretion. The proposed principles are based on the unique characteristics of data regarding minors, on their ability and capacity to make decisions regarding disclosure and publication of such data, and on the role their parents (or legal guardians) with respect to such decisions.

The proposed guidelines include, *inter alia*, the following principles:

- A general obligation to employ privacy by design principles (ie designing privacy and data protection compliance into data systems from the start) in a manner designed to protect minors and minimise the risk to their privacy.
- A prohibition on acts which exploit the weaknesses of minors and on the collection of data which is not necessary for the purposes of the said service or product.
- Prohibition on collecting data on minors under the age of 14, and sensitive data on minors under the age of 18, without parental consent. The prohibition will apply fully to anybody specifically soliciting data from minors, and will impose a duty of care on those soliciting information generally (as opposed to specifically from minors) to meet the above requirements only when there is a reasonable basis that data is being collected from minors.
- At the time of receiving the consent, an obligation to convey clear and concise information to the parents and minors as to the requested use of the data, so to allow 'informed consent' to the use of the data.
- Obliging suppliers who collect data concerning minors to draft a 'privacy policy' and a clear abstract of this document.
- Prohibition on the publication of data which enables the identification of a child minor under the age of 14.
- Deletion of data once it is no longer necessary or at the request of the minor or parent.
- Allowing the database owner to prove compliance with the said principles by examination of an independent auditor.

The Consumer Protection Regulations (Advertisement and Marketing Directed at Minors) 1991 prohibit advertising or marketing which utilises a minor's personal information or personal information regarding a third party obtained from a minor, without the consent of a parent or guardian. 'Personal information' in this context includes the name, address, email address, telephone number or bank account or credit card information. However, the use of personal information in order to provide the goods or services to the minor is permitted.

The Incorporation of Biometric Identification and Data in Identification Documents and in Databases Regulations 2011 (Biometric Regulations) include provisions which limit the collection and use of biometric identification data from minors. Regulation 9 of the Biometric Regulations prohibits collecting fingerprints for purposes of obtaining biometric identification data from a minor below the age of 12. Regulation 2 restricts collecting biometric identification data directly from a minor below the age of 14, and stipulates that only the minor's legal guardian may provide such data.

#### **4.7 Whistleblowing**

Two laws pertain to whistleblowing activities: the Protection of Employees (Exposure of Offences, Unethical Conduct or Improper Administration) Law 1997 (the 'Employee Protection Law') and the Encouragement of Ethical Behaviour in the Public Sector Law 1992 (the 'Ethical Behaviour Law'). The Employee Protection Law applies to employees in both the public and private sectors, and prohibits an employer or supervisor to terminate an employee's employment or impair an employee's employment conditions as a consequence of the employee's allegations of legal violations by the employer.

The Ethical Behaviour Law applies only to public employers and establishes record keeping and reporting requirements with respect to employees' allegations of corruption or unethical behaviour.

There are no unique security standards, retention periods or registration requirements which apply to whistleblowing. Standard data protection principles apply to collection, use and transfer of whistleblowing information.

#### **4.8 Email, Internet and video monitoring**

Monitoring activities are highly regulated in the employment arena (see discussion below). Other monitoring activities are 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 the persons' consent.

In 2012, ILITA issued Directive 4-2012 addressing video monitoring in public places. While Directive 4-2012 primarily addresses video monitoring by public authorities, due to the practical difficulties involved in obtaining the persons' consent to video monitoring, said Directive 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 Directive 4-2012 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 said Directive, 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 invasion of privacy rights;
- the video monitoring must be implemented in a manner that causes least invasion of privacy, utilising the 'privacy by design' model (eg where cameras are situated, times during which they are activated, resolution etc);
- the public must be notified of video monitoring activities (eg using appropriate signage);
- the video images obtained must be kept for a limited time period, which period is consistent with the proportionality test, and is appropriate in light of the purpose to be achieved by recording and the sensitivity of recorded information;
- with respect to persons' inspection rights for materials obtained through video monitoring, the person will generally not have the right to inspect such materials unless the videos are retained for longer than 30 days, the person's image is included in the database, the request is specific and concrete and no third parties are harmed by such inspection; and
- appropriate security measures are taken to secure the information obtained through video monitoring, in accordance with the Privacy Law and Regulations.

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

Israel's highest labour court recently issued a decision which establishes for the first time comprehensive rules regarding employers' monitoring of employees' computer, IT and email use at the 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, IT 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 (eg 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 (eg 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.

In two recent cases deliberated in Israeli labour courts, the question of video monitoring in the workplace was addressed. The court ruled that installing and operating a security camera in employees' workspace without their consent and notwithstanding their express objection constitutes a violation of their privacy. In addition, such practice constitutes significant aggravation in their working conditions, which entitles the employees to resign without such resignation being deemed breach of contract (Civ File 39840-04-10 *Leshziner v Pe'er Medical Rehabilitation Center Ltd* 2011). Another case held that installing security cameras in public areas of the workplace (such as the building entrance) does not constitute a violation of the employees' privacy (Civ File 1116-02-12 *Gafner v Prigo Israel Agencies Ltd* 2013). Additionally, the Eavesdropping Law 1979 prohibits eavesdropping upon 'conversations', which include various sorts of telecommunications, including communications between computers and communications by wireless, optical or electromagnetic means. Thus, monitoring emails without the consent of the writer or recipient may in certain cases constitute a violation of the Eavesdropping Law 1979.

#### **4.9 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 provisions regarding direct mail and direct mail services apply to a broader class of data than the other of database provisions of the Privacy Law and apply to any '*information relating to a person's private affairs*', even if not included under the definition of 'data'. 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 was received and the persons to whom the data was given.

Approaches by direct mail must identify the communication as a direct mail solicitation and include specific information, including: the registration number of the database; that the recipient of the solicitation has the right to be deleted from the database and the address to be contacted for this purpose; the identity and address of the database containing the data from which the solicitation was made; and the sources from which the owner of the database received that data.

In July 2013, the Registrar published a draft directive regarding the interpretation and implementation of the provisions of the Privacy Law with respect to direct mail and direct mail services. While the draft guidelines do not have the status of binding law, they demonstrate what the Registrar views as appropriate interpretation of the provisions of the Privacy Law. The draft directive clarifies that if the solicitation is transmitted to an active customer of the database owner, it is sufficient to only include information about the right to deletion in the solicitation.

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/her or that data 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. The draft guidelines clarify that the Registrar will not enforce the right to be deleted from a database used for direct mail where solicitations are transmitted to all of the database owner's active customers, provided the database owner does not use any sub-categorisations or additional profiling beyond the fact that the customer is an active customer.

In December 2008, Israel enacted Amendment No. 40 to the Israeli Communications Law (Bezeq and Broadcasting) (the '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 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 certain information, including 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).

In a recent case, an Israeli district court authorised the initiation of class action against service providers who have violated the Communications Amendment. In the decision, the court ruled that the practice of automatically calling a phone number and immediately disconnecting in order to induce the customer to call back violated the Communications Amendment. The decision also held that the practice of offering a recipient the opportunity to participate in a quiz for which prizes are awarded, a practice frequently used to obtain contact information for use in disseminating promotional messages, violates the Communications Amendment (Civ File 1586/09 *Hayut v Teleran Instant Messages Ltd Tak-Mehoz* 2011).

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 data using cookies and use of such data.

#### **4.10 Big data**

Not applicable.

#### **4.11 Mobile apps**

A paper titled 'Retention and Use of Location Data in Smartphones' submitted to the Knesset Science and Technology Committee in November 2011 referred both to retention and use of location data by smartphones as well as by the applications downloaded onto smartphones. The paper



proposed the following guiding principles for regulators and legislators with respect to the collection, retention and use of location data:

- (i) Transparency: the end user has the right to receive full, clear and understandable information regarding what data is collected about him/her, especially with respect to location data.
- (ii) Choice: the end user needs to be provided with the ability to choose whether location data is collected from him/her. This choice needs to be more nuanced than 'all or nothing'.
- (iii) Restrictions on the scope of data collected: data collected by smartphones and applications should be restricted. The restrictions should be with respect to the kind of data to be collected, the level of detail of such data, its scope, the justification for the data collection and the anonymity of the data.

## **5. DATA-QUALITY REQUIREMENTS**

Owners, holders and managers of databases are each responsible for data security, and 'data security' is defined to include, among other things, 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 section 10.2 below.

## **6. OUTSOURCING**

### **6.1 Outsourcing**

Outsourcing activities generally implicate the Privacy Law provisions applicable to databases, 'database holders' (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 said 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 person, 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 affect other obligations existing under law.

## **6.2 Due diligence**

Not applicable.

# **7. INTERNATIONAL DATA TRANSFERS**

## **7.1 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 persons 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.

## **7.2 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 is transferred to a country the laws of which ensure that the transferred data is 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 it was received;
  - (iii) stored data shall be correct and current;
  - (iv) persons shall have the right to view and correct the data; and
  - (v) proper security precautions should be implemented to protect the data;
- the person has consented to the transfer;
- the transfer is critical to the person's health and he/she is unable to give consent;
- the data is transferred to a corporation in which the owner of the Israeli-based database has a controlling interest (ie more than 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 has been lawfully publicised;
- the transfer of the data is necessary for the benefit or the security of the public;
- the transfer of the data is required under Israeli law; or
- data is 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 EU 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 cooperative understanding.

### **7.2.1 Data transfer 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 persons 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.

### **7.2.2 Binding corporate rules**

Not applicable.

### **7.2.3 Safe Harbour**

Not applicable (but see section 7.2 above).

### **7.2.4 Other legal bases**

Not applicable.

## **7.3 E-discovery and law enforcement requests**

The Data Transfer Regulations permit international data exports pursuant to the Interstate Legal Assistance Law 1998, which governs data disclosure procedures between Israel and applicable countries in the context of legal proceedings.

## **7.4 Representative**

Not applicable.

# **8. 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 person.

### **8.1 Who**

Any person or entity soliciting information for inclusion in a database is required to provide notice.

### **8.2 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 is requested; and
- (iii) to whom the data will be delivered and for what purpose.

### **8.3 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.

### **8.4 When**

The Privacy Law does not expressly require provision of notice within a specified time frame.

### **8.5 How**

No specific form of notice is required.

## **9. RIGHTS OF INDIVIDUALS**

### **9.1 Who**

As noted in section 1.3.1 above, the rights of inspection and correction of database information are accorded solely to natural persons. The Privacy Law does not require that the person be a resident or citizen of Israel.

### **9.2 What**

If a person's inspection reveals that database information is inaccurate, incomplete, unclear or not up to date, the person may request that the database owner (or, if the owner is a foreign resident, the database holder) correct or if applicable, delete the data. Following correction, the database owner must communicate the correction to anyone who received the data from the database owner within the preceding three-year period.

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 data about him/her from the database. In addition, recent non-binding communications originating from the Registrar derived from the Privacy Law require that database information be deleted when its intended purpose has expired.

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/her 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.

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

### 9.3 Exceptions

The right of access does not apply where:

- the data concerns 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 is privileged (eg 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:

- certain databases maintained by public entities, including databases of security authorities (eg the police, the military police of the Israel Defence Forces, the General Security Service and the Institute of Intelligence and Special Assignments);
- data to which the security of the state, its foreign relations or the provisions of any enactment require that it 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 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 the Prohibition of Money Laundering Law 2000, which contains a record of all reports of money laundering submitted to the Ministry of Justice.

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 data 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).

#### **9.4 When**

Inspection must be permitted within 30 days of the person's request, although the Registrar may extend the period by an additional 15 days. With respect to correction, 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.

#### **9.5 How**

The Privacy Law provides that a person may inspect any information about him/her 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 printout of the requested information in lieu of permitting inspection of the data within the database. The person viewing the printout may not remove the printout from the premises of the database owner or holder without permission.

#### **9.6 Charges**

The owner or holder of the database is entitled to impose a fee of NIS 20 (approximately EUR 4) for the inspection.

### **10. SECURITY OF DATA PROCESSING**

#### **10.1 Confidentiality**

Data 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.

#### **10.2 Security requirements**

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 Regulations, maintaining database security includes:

- ensuring the physical protection of the automatic data processing system and infrastructure;
- setting administrative procedures regarding permitted access to the data and instructions regarding its collection, verification, processing and distribution;
- establishing operating procedures for the system, including data security and protection for the integrity of data;
- implementing reasonable security measures, in accordance with the level of sensitivity of the data; and
- 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:

- the database must be administered according to guidelines for security and supervision of physical storage of the data;
- any printouts 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;
- the database manager must maintain a list of the users of the restricted data, and a list of those permitted access to the data; the access codes must be changed periodically;
- restrictions on access to the backup copies of restricted data;
- documents and magnetic records of intermediate data processing activities must be burned, shredded or otherwise destroyed; and
- 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 individuals can remotely access data stored in a database, the database owner must implement specific verification processes.

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 non-profit IT and information systems professional organisation)) has 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](http://www.justice.gov.il/NR/rdonlyres/C0681561-6CD4-4A6E-AE85-E2ABACC2C171/0/parta.pdf).

### **10.3 Data security breach notification obligation**

Data security breach notification to the authorities is not required under

the current law and, as such, notifications of data security breaches are uncommon; however, if the draft Protection of Privacy Regulations (Information Security in Databases) 2012 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 of security breaches to the database owner. 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 6.1 above).

#### **10.3.1 Who**

ILITA's Directive 2-2011 on outsourcing requires service providers to provide breach notifications to the database owner. The said Directive does not specify which person employed by the service provider must make the notification.

Under the draft Protection of Privacy Regulations (Information Security in Databases) 2012, the security administrator (whether the database manager or a specially appointed security officer) would be required to report directly to either the database owner, the database manager or to a senior officer in order to confirm his/her professional independence. In the scope of his work, he/she would be required to draft a data security procedure, which would be binding upon all the employees having access to the databases. This procedure would include provisions for the report to the database owner of security breaches of medium- to high-security databases. If the draft is enacted as law, in the event of a serious breach of medium- or high-security databases, the database owner would be required to report the incident immediately to the Registrar and identify the steps taken following the event/breach.

#### **10.3.2 What**

Under ILITA's Directive 2-2011, outsourcing notifications must be made of potential security failures, including use of the database not in compliance with agreed data access authorisations.

Under the Protection of Privacy Regulations (Information Security in Databases) 2012, if enacted, notification of the occurrence of the unauthorised use of a high-security database or the unauthorised use of a material portion of the data in a medium-security database would be made to the Registrar.

#### **10.3.3 Exceptions**

Not applicable.

#### **10.3.4 When**

Under ILITA's Directive 2-2011 on outsourcing, notices of breaches must be made immediately.

Under the Protection of Privacy Regulations (Information Security in



Databases) 2012, if enacted, the preferable means for documentation of events of a potential breach of the database would be by automatic documentation. Notification of a serious breach of medium- or high-security databases would need to be made immediately.

#### **10.3.5 How**

Under ILITA's Directive 2-2011 on outsourcing, notices of breaches must be made to the database owner.

Under the Protection of Privacy Regulations (Information Security in Databases) 2012, if enacted, in the event of a serious breach of medium- or high-security databases, the database owner would be required to report the incident to the Registrar and identify the steps taken following the event/breach. The Registrar would have the authority to instruct the database owner to notify affected persons of the breach.

### **10.4 Cybersecurity**

In 2011, the Israeli government passed a resolution to promote national security in cyberspace. Pursuant to such resolution, the 'National Cyber Bureau' was established in 2012. The National Cyber Bureau's responsibilities include making recommendations to the Prime Minister with respect to a national cyber policy, supervising the implementation of such policy, making recommendations with respect to the regulation of cybersecurity and promoting research and development in the cyber field.

An opinion paper prepared by the Knesset Center for Research and Information in 2013 highlights the connection of cybersecurity and the activities of the National Cyber Bureau to the Privacy Law, emphasising that the implementation of cybersecurity policies and responses to cyberattacks may infringe on privacy rights of individuals as well as other constitutional principles (such as freedom of expression, freedom of information and the transparency of the Internet network). No recommendations regarding a national cyber policy or regarding the regulation of the cyber field have been issued to date.

## **11. DATA PROTECTION IMPACT ASSESSMENTS, AUDITS AND SEALS**

Such assessments and audits are recommended in certain circumstances pursuant to the Outsourcing Directive, Directive 4-2012 and the non-binding guidelines published by the Registrar (see sections 4.6, 4.8 and 6.1 above).

## **12. 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.

## **12.1 Notification requirements**

### **12.1.1 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.

### **12.1.2 What**

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

- contains data about more than 10,000 people;
- contains sensitive data;
- contains data about natural persons not provided by them, on their behalf or with their consent;
- belongs to a public body; or
- is used for direct mail services.

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

### **12.1.3 Exceptions**

Even where one of the conditions above is 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.

### **12.1.4 When**

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

### **12.1.5 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 ILITA website, <http://goo.gl/5Iqm7R>. 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 data is intended;
- the types of data to be included in the database;

- details regarding transfers of data; 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 persons.

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 (liable to be) used for, or as a cover for, illegal activities or the data included in the database was 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.

#### **12.1.6 Charges**

Pursuant to the Privacy Regulations (Fees) 2000, as amended in January 2014, the initial fee for database registration is NIS 266 (approximately EUR 55). 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 995 (approximately EUR 210) if the database contains sensitive data concerning more than 10,000 people; NIS 531 (approximately EUR 110) for sensitive data concerning 10,000 people or less; and NIS 266 (approximately EUR 55) 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 265 (approximately EUR 55). Special discounts are granted to owners of multiple databases.

#### **12.2 Authorisation requirements**

Not applicable.

#### **12.2.1 Who**

Not applicable.

#### **12.2.2 What**

Not applicable.

#### **12.2.3 Exceptions**

Not applicable.

#### **12.2.4 When**

Not applicable.

#### **12.2.5 How**

Not applicable.

#### **12.2.6 Authorisation fees**

Not applicable.

### **12.3 Other registration requirements**

Not applicable.

## **12.4 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).

## **13. DATA PROTECTION OFFICER**

### **13.1 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; 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.

### **13.2 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.

## **14. ENFORCEMENT AND SANCTIONS**

### **14.1 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 and can order the destruction of data and databases.

## 14.2 Sanctions

The Registrar may impose the following administrative fines:

- using, holding or managing an unregistered database requiring registration in breach of the Privacy Law: NIS 2,000 (approximately EUR 420);
- use of database information for purposes differing from those for which the database was registered: NIS 5,000 (approximately EUR 1,050);
- delivering false information in a database registration application: NIS 2,000 (approximately EUR 420);
- failing to deliver information or delivering false information in a notice soliciting information for inclusion in a database: NIS 3,000 (approximately EUR 630);
- failing to comply with persons' inspection rights: NIS 3,000 (approximately EUR 630);
- granting access to a database to someone not authorised under the written agreement between the person and the database owner: NIS 3,000 (approximately EUR 630);
- failing to deliver documents or an affidavit to the Registrar where required by a holder of at least five databases: NIS 2,000 (approximately EUR 420);
- failing to appoint a security officer for data security for databases which are so required by law: NIS 3,000 (approximately EUR 630);
- managing or possessing a database used for direct mail services without designating such use in the database registration: NIS 3,000 (approximately EUR 630);
- managing or possessing a database used for direct mail services without properly tracking of sources of information used: NIS 2,000 (approximately EUR 420); and
- managing or possessing a database used for direct mail services without properly notifying the persons concerned or responding to requests for removal: NIS 3,000 (approximately EUR 630).

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.

## 14.3 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; and
- use of data 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 (up to approximately EUR 54,200).

## **15. REMEDIES AND LIABILITY**

### **15.1 Judicial remedies**

An infringement of privacy is actionable as a civil wrong pursuant to the Privacy Law, and a claimant may obtain monetary compensation or injunctive relief. Certain violations of the Privacy Law (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 (approximately EUR 10,500) without proof of damages for breach of privacy rights, and damages may be doubled where the privacy infringement was with intent to harm.

### **15.2 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).

### **15.3 Liability**

Violators may be subjected to five years' imprisonment for disclosing data obtained by virtue of his/her position as an employee, manager or holder in respect of a database, except for the purpose of performing his/her 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:

- managing, possessing or using a database in breach of Privacy Law (ie the obligations to register certain databases);
- delivering false details in an application for registration of a database in violation of the Privacy Law;
- failing to deliver details or delivering false details in a notice attached to a request for information under the Privacy Law;
- failing to comply with the provisions of the Privacy Law, regarding the right to inspect information kept in a database or failing to amend a database in accordance with the requirements of the Privacy Law;
- 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;
- failing to appoint a Security Officer for data security as required by the Privacy Law;
- managing or possessing a database used for direct mail services in breach of the provisions of the Privacy Law regarding direct mail; and
- 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 2 (protection of privacy in a database) or Chapter 4 (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.

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

**UNITED KINGDOM**

Daniel Cooper  
Covington & Burling LLP  
265 Strand  
London WC2R 1BH  
UK  
T: +44 20 7067 2000  
F: +44 20 7067 2222  
E: dcooper@cov.com  
W: www.cov.com

**UNITED STATES**

Kurt Wimmer  
Covington & Burling LLP  
1201 Pennsylvania Avenue, NW  
Washington, DC 20004-2401  
US  
T: +1 202 662 5278  
F: +1 202 778 5278  
E: kwimmer@cov.com  
W: www.cov.com