

ISRAEL

Barry P Levenfeld and Yoheved Novogroder-Shoshan*
Yigal Arnon & Co, Jerusalem, Israel

CONTENTS

- 1 Introduction
- 2 Scope of law and definitions
- 3 Obligations of data controller
- 4 Obligations of processing bureaux
- 5 Obligations relating to disclosure and transfer of data
- 6 Rights of data subjects
- 7 The regulatory body
- 8 Offences and enforcement
- 9 International aspects and the future
- Annex List of primary and secondary legislation

* The authors are grateful to Arye Schreiber and Avigail Frisch for their extremely valuable assistance.

1 INTRODUCTION

1.1 Title of legislation and amendments

Data protection in the State of Israel is governed primarily by the Protection of Privacy Law 1981 ("the Privacy Law"), and in particular by Chapter Two of that law, which is entitled "Protection of Privacy in Databases".

Chapter Two of the Privacy Law was changed significantly by a 1996 amendment ("the 1996 amendment") which, among other things, addressed procedures for registering databases, authorised the Registrar of Databases to refuse registration in certain circumstances, established the role of the database manager, excluded certain data stored on personal computers from registration requirements and added a new sub-chapter dealing with direct mail solicitations. Other amendments and certain orders are listed in the Annex to this chapter.

1.2 Date in force

Chapter Two of the Privacy Law came into force on September 12, 1981. The 1996 amendment came into force in most respects on October 12, 1996. The dates that other amendments and secondary legislation came into force are set out in the Annex to this chapter.

1.3 Broad scope of legislation

The underlying purpose of the Privacy Law is to protect the privacy of individuals by regulating the storage and dissemination of information relating to such individuals.

1.4 Brief summary of the main provisions of privacy law

- (1) Limiting the publication or use of data concerning a person's private affairs.
- (2) Requiring the registration of databases with the Registrar of Databases, and set out the prerequisites for such registration.
- (3) Setting out regulations regarding the operation and management of databases, including the requirement to respect certain rights of the data subjects.
- (4) Establishing the Registry of Databases ("the Registry") and the rights and duties of the Registrar of Databases ("the Registrar").

1.5 Brief history

The concept of data protection is rooted in the general right to privacy. The right to privacy has been recognised by the Supreme Court in Israel as a fundamental right and since 1992 has been anchored in the quasi-constitutional Basic Law: Human Dignity and Liberty ("the Basic Law"). The Basic Law 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" (s.7 of the Basic Law).

Prior to the enactment of the Basic Law, the Parliament enacted the Privacy Law. The Privacy Law prohibits an infringement of the privacy of any person without that person's consent and provides for both civil and criminal liability for an infringement of privacy (ss.1 to 5). In this context, "person" is defined as natural persons only, and does not include legal entities. The Privacy Law, as originally enacted, included provisions on data protection, and established the position of Registrar of Databases, but it is widely acknowledged that, even at the time of its enactment, the Privacy Law provisions concerning databases were technologically outmoded.

During the years following the enactment of the Privacy Law, it became clear that the protection offered by the Privacy Law was insufficient, that there were significant leaks of information from databases and that private information was held in databases that were easily accessible by persons without a legitimate right to access

such data. The Privacy Protection Council, which advises the Ministry of Justice, prepared an amendment to the Privacy Law in 1993 in order to increase the protection of privacy of data. That effort gave rise to the 1996 amendment and other amendments discussed elsewhere in this chapter.

2 SCOPE OF LAW AND DEFINITIONS

2.1 Scope of data regulated

2.1.1 General right to privacy

Section 2 of the Privacy Law lists 11 activities which constitute an infringement of privacy if carried out without consent. Six of these activities are relevant to data protection and the scope of data regulated:

- (1) copying a letter or electronic message not intended for publication or use of its contents without the permission of the sender or the recipient, provided that the letter or electronic message does not have historic value and fifteen years have not passed from the date it was written (s.2(5));
- (2) infringing an obligation of secrecy laid down by law in respect of a person's private affairs (s.2(7));
- (3) using, or passing on to another, information on a person's private affairs, other than for the purpose for which it was given (s.2(9));
- (4) publishing or passing on anything that was obtained by way of an infringement of privacy under paras (1) and (2) above (s.2(10));
- (5) infringing an obligation of secrecy laid down by explicit or implicit agreement in respect of a person's private affairs (s.2(8)); and
- (6) publishing any matter that relates to a person's intimate life, state of health or conduct in "the private domain" (s.2(11)).

Therefore, in broad terms, any kind of information without regard to how it is maintained or to its content is governed by the Privacy Law to the extent that the use of the information constitutes an infringement of a person's privacy. It is important to note that there are numerous other laws imposing obligations of secrecy which, if breached, could constitute an infringement of privacy under s.2(7) and (8), such as the Banking Ordinance 1941, the Patients' Rights Law 1996 and the Income Tax Ordinance (new version).

2.1.2 Protection of privacy in databases

Chapter Two of the Privacy Law regulates the protection of privacy in databases.

“Data” is defined in s.7 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. In considering whether a bank had a right of access to information about pledges in a governmental database that was maintained by reference to vehicle registration numbers, the Supreme Court held that the term “data” must be interpreted in accordance with the legislative purpose of the Privacy Law. Even though the data was not classified by the personal names of the individuals, but rather by vehicle number, and therefore arguably did not constitute information about a *person*, the court held that since it was possible to derive information about “the economic situation” of a person from the information (and the economic situation of a person was a category of information which was deemed “data” and protected by the Privacy Law), the information was deemed to be “data”. See *State of Israel v Bank Hapoalim Ltd* (1989) 44 (ii) PD 726.

The 1996 amendment added the term “sensitive data”, defined as details regarding a person's personality, private affairs, state of health, economic situation, opinions and faith, and other information deemed to be sensitive data by order of the Minister of Justice with approval by the Constitution, Law and Justice Committee of the Knesset (see 3.4 below). In addition, the regulations created a third category of data called “restricted data”, which includes data about a person's health and data related to the security, defence and foreign affairs of the State of Israel. Special procedures apply with respect to the management of databases containing restricted data and the use of such information; see the Protection of Privacy Regulations (Conditions for Possessing and Protecting Data and Procedures for Transferring Data between Public Bodies) 1987, regs 1 and 8–15 (“the Data Possession Regulations”), and 3.11 below.

A “database” is defined in s.7 of the Privacy Law as “a collection of data, stored by magnetic or optical means and intended for computer processing”, excluding the following two specific kinds of databases:

- (1) any collection of data for personal use that is not used for business purposes (s.7). Prior to the 1996 amendment, the definition of “database” included, broadly

speaking, information held by any person on a home computer. Such a person was required to register the computer with the Registrar and could have been subjected to sanctions if he failed to do so, even if the computer was used solely for personal and family uses. The explanatory notes to the proposed law state that this requirement was one that the public simply could not meet. See Explanatory Notes to Proposed Law, *Reshumot, Hatza'at Hok* 2234 (1994) at page 148. Therefore, the 1996 amendment provided that databases held solely for personal use were excluded from the definition of “database”; and

- (2) a collection of data that contains only names, addresses and means of communicating with the data subject (e.g. telephone and 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 (s.7, Privacy Law). The purpose of this exclusion was to ensure that any collection for business purposes used solely to maintain contact with customers would not require registration. See *Reshumot, Hatzat Hok* 2234 (1994) at p.148.

2.2 Scope of regulated processing activities

Although the definition of "database" requires that the data be "kept by magnetic or optical means and intended for computer processing", the Privacy Law does not define the term "computer processing". It does, however, set out in general terms the types of activities which, if performed with respect to data, would constitute a breach of the Privacy Law, these include:

- (1) using or passing on to a third party data otherwise than for the purpose for which they were given (s.2(9));
- (2) publishing or passing on anything that was obtained by way of an infringement of privacy (s.2(10)); and
- (3) publishing any matter that relates to a person's intimate life, state of health or conduct in the private domain (s.2(11)).

2.3 Scope of protected data subjects

Although 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 (s.3), 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 in Israeli law (Eli Halm *Privacy Law* (Perlstein, Israel 2003) pp.157 et seq.). Also, the definitions of "data" and "database" (see 2.1 above) indicate that the provisions of the Privacy Law that specifically regulate databases (Chapters Two and Four) apply only to databases containing information about natural persons. Finally, the rights to inspect information in a database and request its amendment or deletion are only granted to individuals (ss.13 and 14). The Privacy Law does not require that the individual be a resident or citizen of Israel.

2.4 Scope of controllers regulated

The Privacy Law and the regulations promulgated thereunder impose specific obligations on database owners, database holders and database managers; these obligations are discussed more fully below.

In addition, all persons or legal entities are prohibited from using data in a database that is required to be registered, other than for the purposes for which the database

was created (s.8(b)). "Use", defined as including "disclosure, transfer and delivery" (s.3), is likely to include processing as well.

The Privacy Law does not define "database owner". A "database manager" is defined as the active manager of the body which owns or possesses a database, or a person authorised to carry on such activities by the manager for this purpose (s.7). A "database holder" is defined as one who has a database in his possession on a permanent basis and is permitted to use it (s.3).

The obligation to register a database is imposed on the database owner (s.8(c)). However, the Privacy law also prohibits the management or holding of a database that is required to be registered if it is not registered (unless the Registrar failed to notify the applicant within 90 days that the registration was denied or delayed, or the requirement to register derives from an order of the Registrar which was permitted to operate prior to registration) (s.8(a)).

There are other provisions that apply specifically to managers and holders of databases (ss.16 and 17), employees (s.16), entities that possess databases of different owners (s.17A(a)), entities that possess five or more databases that require registration (s.17A(b)), public bodies holding databases (s.17A(a)), and banks, insurance companies and companies engaged in ranking or evaluating credit ratings (s.17B).

2.5 Application to processing bureaux

There are requirements applicable to "external service providers" in the provisions governing data security (see 3.11 below) and one provision relating to a "service bureau" in the regulations governing inspection of data by data subjects (see 6.1 below).

The original version of the 1996 amendment that was prepared by the Privacy Protection Council contained a number of special provisions concerning service bureaux, but these provisions were not included in the amendment as adopted. See *Reshumot, Hatza'at Hok 2234* (1994) at page 148. The intention of the provisions was to regulate the growing number of data processing service providers which have the potential to gather considerable amounts of data. Although the provisions relating to the specific category of "service bureaux" were not adopted, other provisions which were adopted essentially achieve the same goal by regulating holders of databases owned by other parties, and holders of five or more databases requiring registration (see 3.9 below and ss.17A(b) and 17B).

2.6 Application to manual records

The definition of "database" requires that the data be "kept by magnetic or optical means and intended for computerised processing" (s.7). Therefore, the database regulation provisions of the Privacy Law do not apply to manual records.

2.7 However, Section 2 of the Privacy Law, which defines specific activities that constitute an invasion of privacy, apply to all data, regardless of the form in which it is maintained, and these provisions apply to manual records as well as electronic records. Thus, the Privacy Law regulates both invasions of privacy generally and

specifically the creation and use of databases, while the Privacy Law's database provisions apply only to data in computerised form, the law's provisions applicable to privacy rights generally apply to all information regardless of the form in which it is maintained.

Chapter Four of the Privacy Law specifically governs the delivery and receipt of data and information to and from public bodies. Section 23A provides that all of Chapter Four applies to any information that relates to a person's "private affairs", even if it does not fall within the definition of "data" (s.23A and Explanatory Notes to Proposed Law, *Reshumot, Hatzat Hok* 1628 (1983) at page 176). In this context, there is no requirement that the data be "kept by magnetic or optical means and intended for computer processing".

2.7.1 Definition of a public body

A "public body" is defined as:

2.7.1.1 government departments and other state institutions, local authorities, and any other body performing lawful public functions; and

2.7.1.2a body designated by an order of the Minister of Justice, with approval of the Knesset's Constitution, Law and Judiciary Committee, so long as the order specifies the categories of information and items the body is entitled to deliver and receive (s.23).

A number of organisations and institutions have been designated public bodies by order for the purpose of collecting specific kinds of data. For example:

- (i) hospitals and health funds (kupot holim) may collect information regarding the health of a person for treatment purposes;

- (ii) higher educational institutions may collect information containing personal details for research purposes; and

- (iii) an organisation that provides assistance to disabled army veterans may collect certain information about disabled veterans.

See the Protection of Privacy Order (Determination of Public Bodies) 1986.

2.7.2 Prohibition on delivering data

In general terms, a public body is prohibited from delivering data unless:

2.7.2.1 the data has been lawfully published;

2.7.2.2 the data has been lawfully made available for public inspection; or

2.7.2.3 the data subject consents to the delivery of the data (s.23B(a)).

2.7.3 However, the Privacy Law provides exceptions to this general prohibition on disclosure in favour of security authorities (e.g. the police) (s.23B(b)) and, subject to compliance with a number of additional obligations, public bodies that deliver information to other public bodies as part of their lawful jurisdiction or tasks (ss.23C and 23D).

The Freedom of Information Law 1998 ("the Freedom of Information Law"), which was enforced in May 1999, establishes the right of Israeli citizens or residents to obtain access to public "information", defined in s.2 as any information found within the public sector which is written, recorded, filmed, photographed or computerised. Pursuant to s.7 of the Freedom of Information Law, if a request is submitted to a government authority, the government authority must provide the requested information within 30 days (which may be extended by additional 30 days) or give written reasons for denying the request.

Certain provisions of the Freedom of Information Law are designed to protect privacy. For example, s.9 provides that a government authority is forbidden to disclose certain information to the public unless permitted pursuant to any law, this includes information that if disclosed would constitute an infringement of privacy under the Privacy Law. Section 13 provides that before disclosing information about a third party which could harm their interests, the government authority must notify the third party about the request for disclosure, and allow 21 days for such person to respond. If the person opposes disclosure but the government authority decides that the information should nonetheless be disclosed, then the government authority must provide a reasoned opinion and an opportunity for such person to appeal the decision before disclosure.

The Freedom of Information Law does not take precedence over other binding legislation which requires, allows or restricts the disclosure or transfer of information from a public body, i.e. the Privacy Law (Freedom of Information Law, s.20).

2.8 General exemptions

As discussed at 2.1 above, databases held solely for personal use or containing exclusively the names, addresses and contact numbers of customers or other business contacts (provided the business does not maintain any other registrable databases) are exempt from the provisions of the Privacy Law because they are excluded from the definition of "database" (s.7).

An exemption provides that no person shall be responsible under the Privacy Law for an act which he or she is empowered to do by law (s.19(a)). This provision broadly encompasses any disclosure of data that a person is authorised to make under any statute, ordinance or regulation. Another exemption provides that no security authority, including the Protection of Witnesses Authority, or person employed by or acting on behalf of a security authority, shall be responsible under the Privacy Law for an infringement reasonably committed within the scope of its functions (s.19(b)).

Additional defences apply in respect of the invasion of privacy, these defences do not however apply to a breach of the database provisions of the Privacy Law. In particular, pursuant to s.18 of the Privacy Law, it is a good defence in criminal or civil

proceedings for infringement of privacy, if the infringement was committed in good faith:

2.8.1 by someone who neither knew, nor should have known, of the possibility of an infringement of privacy;

2.8.2 in circumstances in which the infringer was under a legal, moral, social or professional obligation to commit the infringement;

2.8.3 in defence of a legitimate personal interest of the infringer; or

2.8.4 in circumstances permitted under the Prohibition of Slander, 1965.

Another defence exists for an infringement of privacy that is justified, in the circumstances, as being in the public interest (s.18(3)). In *Registrar of Databases v Moshe Ventura* (1988) 48 (iii) PD 808, the Supreme Court held that the public interest in obtaining information about cheques, bills of exchange and other financial obligations that had not been honoured was not sufficient to justify the invasions of privacy and potential harm likely to be caused to the individuals, and upheld the Registrar's refusal to register a database intended for the collection and disclosure of data about dishonoured cheques. However, subsequent to the issuance of the verdict, a limited version of the database in question was indeed registered, and certain restrictions were imposed regarding inspection rights of the data subjects with respect to such database.

2.9 Application to journalistic activities

Journalistic activities are not exempt and are subject to all the provisions of the Privacy Law.

2.10 Other relevant definitions

The term "publishing", used in s.2(10) and (11), is broadly defined to include any means of communication, whether oral, written or printed "and all other means" (s.3 of the Privacy Law, adopts the definition of "publishing" from s.2 of the Defamation Prohibition Law 1965). Furthermore, included within the definition of "publishing" is a provision stating that publishing includes material that is "intended for a person (other than the injured person) and which is received by that person or by any person other than the injured person" and "written and the writing is likely, in the circumstances, to be received by any person other than the injured person" (s.2 of the Defamation Prohibition Law 1965).

3 OBLIGATIONS OF THE DATA CONTROLLER

3.1 Registration and notification requirements and procedures

Section 8(c) of the Privacy Law requires the owner of a database to register the database if any of the following conditions is met:

3.1.1 the database contains data about more than 10,000 people (see definition of "data" at 2.1 above);

3.1.2 the database contains sensitive data (see definition of "sensitive data" at 3.4 below);

3.1.3 the database contains data about natural persons not provided by them, on their behalf or with their consent;

3.1.4 the database belongs to a public body (see definition of "public body" at 2.7 above); or

3.1.5 the database is used for direct mail (see definition of "direct mail" at 3.10 below).

Further to a 2007 amendment, "consent" means informed consent, and consent may be 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 purposes of providing consent.

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 lawful authority (s.8(d)). 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 by virtue of s.8(c) and (d) must nonetheless be registered (s.8(e)).

Applications to register a database must be submitted to the Registrar (s.9). The application must specify the following:

(1) the identity and address in Israel of the owner of the database, the person with possession of the database and the manager of the database;

(2) the purpose for setting up the database and the purposes for which the information is intended;

(3) the types of data to be included in the database;

(4) details regarding transfers of data outside the borders of the state;
and

(5) 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 any entity which owns a database must notify the Registrar in writing of the name of the database manager for inclusion in the Registry (see reg.2 of the Data Possession Regulations).

At the time of writing, pursuant to the Privacy Regulations (Fees) 2000, as amended in December 2010 and January 2011, the initial fee for database registration was 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 on the basis of 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.

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 (s.9(d) of the Privacy Law).

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:

(1) the database is used or is liable to be used for illegal activities or as a cover for illegal activities; or

(2) 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 (s.10(a)(1) of the Privacy Law).

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 (s.10(a)(2)).

If the Registrar does not register the database within 90 days and does not inform the applicant registration has been refused or delayed, then the applicant is permitted to operate the database even if it is not registered (s.10(b1)). However, if the Registrar does inform the applicant of a refusal or delay in registration, then the applicant may not manage or possess the database, unless a court decides otherwise (s.10(b2)).

All of the details required to be included in the application for registration pursuant to s.9 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) (ss.12 and 13).

3.2 Conditions to be met for holding and processing of data

Possessing or managing a database that must be registered is prohibited unless:

3.2.1 the database has been registered (s.8(a));

3.2.2 the application to register the database has been submitted and the Registrar has not registered it within 90 days and has not notified the applicant of a refusal to register or a delay for special reasons (s.10(b1)); or

3.2.3 the Registrar has issued an order stating that the database must be registered (in respect of a database that would not normally be subject to the registration obligation) and the Registrar's order grants permission to manage and possess the database during the registration procedure (s.8(e)).

3.3 General principles relating to processing of data

The only general principles relating to processing of data are those forming part of the obligations governing data security discussed in 3.11 below. They include the obligation to set up administrative procedures applicable to an external service provider that provides data processing services, and the requirement to destroy any intermediary print-outs from data processing involving "restricted data" (see 3.4 below).

3.4 Specific provisions relating to sensitive data

"Sensitive data" is defined as details regarding a person's personality, private affairs, state of health, economic situation, opinions and faith, and other information deemed to be sensitive data by order of the Minister of Justice with approval of the Constitution, Law and Justice Committee of the Parliament (s.7). A comparison between the definitions of "data" and "sensitive data" reveals the following differences: "sensitive data" does not include data regarding a person's personal status and professional qualifications; and the concept of "sensitive data" can be expanded by an order not requiring a statutory amendment. To date, there have not been any orders expanding the definition of "sensitive data".

Any database that contains "sensitive data" must be registered in the Register of Databases by means of an application to the Registrar submitted by the database owner (ss.8(c)(2) and 9).

In addition to the term "sensitive data" in the Privacy Law, the regulations create another category of information called "restricted data", which is defined to include data about a person's condition of health (see reg.1 of the Data Possession Regulations). In order to ensure that the security of "restricted data" is maintained,

Chapter Four of the Data Possession Regulations sets out a number of requirements for the management of any database that contains "restricted data" (see 3.11 below).

3.5 Specific provisions relating to medical data

There are a few provisions that relate specifically to medical data, all of the provisions regarding databases also apply to databases containing medical data because information regarding a person's condition of health falls within the definitions of both "data" and "sensitive data" (s.7). Thus, any database that contains information about a person's health condition must be registered (s.8(c)(2)).

In addition, medical information is among the subjects deemed to be "private affairs" for the purposes of s.2(7) and 2(8). The effect of this is that infringement of the obligation of secrecy could constitute an infringement of privacy subjecting the infringer to civil penalties, and to criminal penalties more stringent than those relating to infringement of database-related requirements (ss.2, 4 and 5 of the Privacy Law).

Furthermore, the regulations governing "restricted data", which requires additional security measures to be taken, are applicable to databases containing data about a person's condition of health (see 3.4 above and 3.11 below).

Finally, a database owner is not required to allow a person to inspect information that relates to his or her physical or mental health if the database owner believes that the information could cause severe harm to the person's health or endanger his or her life. The information must, however, be given to the person's physician or psychologist (s.13(c)).

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.

It should also be noted that a number of other laws and directives impose on care-providers, employees and medical institutions an obligation of secrecy regarding patient information. For examples, see the Patients' Rights Law 1996, the Treatment of the Mentally Ill Law 1991 and the Psychologists' Law 1977. In addition, in 2007, the Ministry of Finance issued a directive which requires insurance companies and employers to maintain the medical secrecy of foreign workers.

3.6 Specific provisions relating to credit data

The collection and dissemination of credit data has been regulated in the Credit Details Service Law 2002 ("the Credit Law"). The law applies both to 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 its database 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.

With regard to credit data, the Credit Law distinguishes between data regarding the subject'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 (s.16, the Credit 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 (s.17, the Credit Law). The registrar must keep a list of subjects who have consented in this manner, and upon request in writing from the subject, must delete the subject 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 (s.21, the Credit Law).

The law contains a number of provisions on the manner in which the data may be collected and disseminated. For example, data may only be held for seven years, after which it must be destroyed (s.20, the Credit Law). 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 (s.28, the Credit Law). The subject of the data is entitled to receive, free of charge and within seven days of request, a credit report relating to himself, inspect the data that pertains to him or her, and may contact the license holder if he or she believes that the data is not true, complete, clear, or current (ss.25, 31, the Credit Law). 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 s.17B(a)(3) of 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 (see the discussion on data security at 3.11 below).

Under s.38(c) of the Credit Law, a transferor of information to a licensed owner of a credit database in accordance with the law is not liable under the Privacy Law.

3.7 Specific provisions relating to other specific types of data

The Privacy Law contains several provisions regarding data relating to the security authorities, defence and foreign relations of the state (for example, see ss.12, 13(e) and 19(b) of the Privacy Law, as well as regs 8 to 15 of the Data Possession Regulations). Although details of these are beyond the scope of this chapter as they relate to the public sector, brief summaries have been provided at 3.11.3 and 6.1.3 below.

3.8 Specific provisions relating to automated decision-making

There are no specific provisions relating to automated decision-making.

3.9 Specific provisions relating to pooling, matching, cross-referencing or profiling

The potential for infringements of privacy arising from cross-referencing and profiling were concerns underlying the 1996 amendment. The explanatory notes to the proposed law (i.e. the draft 1996 amendment) discuss the importance of protecting privacy in light of the growing sector of the economy that provides automatic data processing services. The explanatory notes comment that the entities providing these services are capable of accumulating many different databases, gathering large quantities of data, and engaging in cross-referencing of the data.

Also, entities involved in providing direct mail services would be able to infringe people's privacy by classifying them into categories based on their personal characteristics, and publicly disseminating these "profiles" without consent. See *Reshumot, Hatza'at Hok* 2234 (1994) at page 148. The proposed law contained a section regulating direct mail services, which was in large part enacted (see 3.10 below and s.17(c)–(i) of the Privacy Law). See also 1.1 above for a summary of the changes introduced by the 1996 amendment.

3.10 Specific provisions relating to direct marketing

Part Two of Chapter Two of the Privacy Law, which entered into force in April 1997, 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" (s.17C).

The Privacy Law prohibits a person from managing or possessing a database that is used for direct mail services unless it is registered in the register and one of its stated purposes is direct mail services (s.17D). This requirement to state the purpose was intended to facilitate supervision of compliance with the provisions regarding direct mail. See *Reshumot, Hatza'at Hok* 2234 (1994) at p.148.

A person who manages or possesses a database used for direct mail services must keep a record stating the source of all of the data, the date the data was received and the persons to whom the data was given (s.17E).

Pursuant to s.17F(a), every direct mail solicitation must state clearly:

3.10.1 that it is a direct mail solicitation;

3.10.2 the registration number of the database;

3.10.3 that the recipient of the solicitation has the right to be deleted from the database and the address to be contacted for this purpose;

3.10.4 the identity and address of the database containing the data from which the solicitation was made; and

3.10.5 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 (s.17F(b)). Also, s.17F(c) provides that every person may demand that personal information is not be given to a specific person, to a category of persons, or to any person at all, whether for a specific period of time or indefinitely. The owner of the database must comply with these requests and give written notice of the fact that he has complied (s.17F(d)). 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 (s.17F(e)).

All of the provisions governing databases used for direct mail apply to other information about a person's "private affairs" to the same extent that they apply to "data" (s.17G). The term "private affairs" is broader than "data" and is included to ensure that the direct mail provisions apply to all information protected by privacy rights (see 2.1.1 above).

A public body performing its tasks under any enactment is not subject to the provisions governing databases used for direct mail services (s.17H).

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 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 themselves offering the goods or services, 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 recipient consent under limited circumstances.

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

(i) 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;

(ii) the advertiser's identity and contact information; and

(iii) 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).

3.11 Security requirements

3.11.1 Definition of data security and responsible parties

The Privacy Law contains specific provisions regarding the security of data in databases. "Data security" is defined in s.7 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 further defined in s.7 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 held individually responsible for data security (s.17).

In the following three situations s.17B(a) requires appointment of a suitably trained person to be in charge of data security ("the Security Officer"):

3.11.1.1 the holder of five or more databases requiring registration under s.8;

3.11.1.2a a public body, as defined in s.23 of the Privacy Law; and

3.11.1.3a a bank, insurance company or a company involved in ranking or evaluating credit.

While the Security Officer is to be responsible for data security, the database owner, holder and manager nevertheless each are held individually responsible under the Privacy Law for data security as well (s.17B(b)). The database manager must inform the Register as to the identity of the Security Officer (reg.2 of the Data Possession Regulations).

3.11.2 Requirements for data security

Maintaining database security includes the following obligations:

3.11.2.1 ensuring physical protection of the automatic data processing system and infrastructure;

3.11.2.2 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);

3.11.2.3granting access authorisation to the database and restricting the access of authorised

users in accordance with the instructions of the Data Transfer Committee (this also applies to public bodies);

3.11.2.4preparation of an updated list of authorised users according to the various degrees of authorisation;

3.11.2.5ensuring the authorised users sign undertakings to maintain the confidentiality of the data and to uphold the instructions established in accordance with paras (2) and (3) above;

3.11.2.6establishing operating procedures for the system, including data security and protection for the integrity of data;

3.11.2.7implementing 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

3.11.2.8establishing controls to reveal damage to the integrity of data and repair defects.

See reg.3 of the Data Possession Regulations.

3.11.3Additional requirements for ``restricted data''

In addition, the Data Possession Regulations set out further requirements for the management and security of any database that contains ``restricted data". The regulations define ``restricted data" as:

3.11.3.1data about a person's health situation;

3.11.3.2data subject to the provisions of s.13(e)(1), (3) and (4) of the Privacy Law (primarily databases related to security, defence and foreign affairs); and

3.11.3.3any other data deemed ``restricted" by an order of the Minister of Justice (no such order has been published as yet).

Any database that contains ``restricted data" is subject to additional security requirements by virtue of the Data Possession Regulations. These obligations include the following:

- (1) 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.);

(2) 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;

(3) 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;

(4) restrictions on access to the back-up copies of restricted information;

(5) documents and magnetic records of intermediate processing activities must be burned, shredded or otherwise destroyed; and

(6) the database manager must keep a journal of atypical events and save it for three years.

See regs 8 to 15 of the Data Possession Regulations.

In addition, in 2010 the Registrar of Databases published Directive 1-2010 which imposes guidelines for identity verification methods to be used when enabling remote access by a data subject to the data subject's personal data stored in a database. The directive requires that the verification process solicit from the data subject 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 alternately, 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 under section 17.

3.11.4 Guidelines for implementing security requirements

The Privacy Protection Council (see 7.5 below) and the Israel Chamber of System Analysts have issued a set of guidelines ("the Guidelines") intended to assist database managers in implementing the Privacy Law. A revised version of the Guidelines was published in September 1999 (and thus does not address the most recent amendments to the Privacy Law). The Guidelines are in Hebrew and contain a summary of the Privacy Law and regulations promulgated thereunder. The Guidelines also explain steps to be taken to ensure data system security, including software and hardware requirements, physical security, and administrative procedures. Annexes to the Guidelines include the full texts of the Privacy Law and the regulations, as well as various forms that may be used for compliance with the Privacy Law. The Guidelines have been posted on the Registrar of Databases website, and may be accessed using the following link: <http://www.justice.gov.il/NR/rdonlyres/C0681561-6CD4-4A6E-AE85-E2ABACC2C171/0/parta.pdf>

3.12 Other relevant obligations of the data controller

Section 11 provides that any request to a person (including a legal entity) to provide data that will be held or used in a database must be accompanied by a notice stating:

3.12.1 whether the person has a legal obligation to deliver the data or whether delivery depends on consent;

3.12.2 the purpose for which the data is requested; and

3.12.3 to whom the data will be delivered and for what purpose.

It should be noted that the intelligent use of these forms of notice may assist in managing business databases and transferring data from registered databases located in Israel to databases located outside Israel and the transfer of data from one legal entity to another, in accordance with s.2 of the Protection of Privacy Regulations (Transfer of Data to Databases outside State Borders) 2001 ("the Data Transfer Regulations"). (See 5 below.)

4 OBLIGATIONS OF PROCESSING BUREAUX

Although the provisions of the proposed law defining and regulating "service bureaux" were not enacted, other provisions of the 1996 amendment, together with the existing provisions of the Privacy Law, effectively accomplish similar results. For example, the 1996 amendment included the following provisions governing anyone who possesses databases with different owners, and anyone who possesses five or more databases that are registrable pursuant to s.8 of the Privacy Law:

4.1 Anyone who possesses a database owned by different owners may not let anyone have access to the database unless that person is explicitly authorised in a written agreement between the holder of the database and the owners of that database (s.17A(a)).

4.2 Anyone who possesses five or more databases that are registrable under s.8 is obligated to appoint a person to be in charge of data security and to submit the following to the Registrar each year:

(a) a list of the databases in his possession;

(b) an affidavit that the persons who are authorised to have access to each database have been specified in agreements between him and the database owners; and

(c) the name of the person appointed to be in charge of data security.

See ss.17A(b) and 17B(a) of the Privacy Law.

5 OBLIGATIONS RELATING TO DISCLOSURE AND TRANSFER OF DATA

5.1 Terminology explained

An infringement of privacy in breach of the Privacy Law can stem from using, passing on or publishing information or data. The Privacy Law does not expressly distinguish between electronic transfers and other means of disclosure.

With respect to databases, the Privacy Law specifically prohibits "the use" of any data in a database that must be registered, other than use for the purpose for which the database was set up (s.8(b)). The term "use" is defined so as to include disclosure, transfer and delivery (s.3) and probably includes processing. Also, the Privacy Law specifically prohibits anyone from disclosing data that was obtained due to his position as an employee, manager or holder in respect of a database, other than for the purpose of performing the person's work or implementing the Privacy Law or in accordance with a court order (s.16).

5.2 Disclosure of data within the same legal entity

While there are a number of provisions that govern disclosures of data (for examples, see 2.1 and 5.1 above, and ss.1, 2 and 16 of the Privacy Law), these provisions do not specifically regulate disclosures of data within the same legal entity. However, disclosures within the same legal entity could constitute an infringement of privacy under the Privacy Law if, for example, the disclosure infringed an obligation of secrecy in violation of s.2(7) or (8), or the information concerns a person's private affairs and was used other than for the purpose for which it was given, in violation of s.2(9). A disclosure within the same legal entity could also constitute a violation of an obligation of secrecy under s.16 of the Privacy Law.

In addition, implementation of the regulations regarding data security and restricted data could, in certain circumstances, require that security measures be taken to prevent unauthorised access to data by persons within the same legal entity (see also 3.11 above). For details, refer to regs 3 and 8–15 of the Data Possession Regulations and pp.20–29 of the Guidelines.

5.3 Disclosure of data to another legal entity

The provisions of the Privacy Law which govern disclosures of data do not specifically refer to disclosures of data to another legal entity. Thus, presumably, all of the provisions regarding disclosures of data are applicable in this context. See, for example, 2.1 and 5.1 above, and ss.1, 2, 8(b), 16 and 17A of the Privacy Law. Note that anyone possessing databases of different owners or at least five databases that require registration must have agreements with the database owners that specify who may be allowed access to the database (see 3.9 above, and s.17A of the Privacy Law). However, there are also a number of defences and exemptions which allow certain

disclosures that would otherwise be prohibited (see 8.1.3 below, and ss.18 and 19 of the Privacy Law).

The Registrar of Databases published an opinion in the annual report for the year 2000 (see 7.2 below) regarding the scope of the prohibition of disclosure of information contained in a database without the consent of the data subjects. The Registrar of Databases is of the view that the transfer of any information contained in a database, whether or not defined as "data" under the Law, is prohibited. This opinion was issued in response to a specific query seeking permission to disclose contact information (names, telephone numbers and addresses) since information of that type, standing on its own, is not considered "data" under the Law. The Registrar of Databases recognises that the position is not supported by the current wording of the statute and proposes that the Law be amended to adopt a wider view of the scope of the prohibition on transfer of information from databases. We are of the belief that the prohibition suggested by the Registrar of Databases is overbroad and unwarranted and that the same result (i.e. the prevention of the disclosure of contact information) can be achieved within the existing Law.

5.4 International electronic transfers of data

Under the Data Transfer Regulation, which came into effect in January 2002, 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, an international transfer may not be made unless one (or more) of the following criteria is met:

5.4.1 the data is 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:

5.4.1.1 data must be gathered and processed legally and fairly;

5.4.1.2 data shall be held, used and transferred solely for the purpose for which it was received;

5.4.1.3 stored data shall be correct and current;

5.4.1.4 subjects of the data shall have the right to view and correct the data; and

5.4.1.5 proper security precautions should be implemented to protect the data;

5.4.2 notwithstanding, data may be transferred in the event that one of the following conditions applies:

5.4.2.1 the subject of the data has consented to the transfer;

5.4.2.2 the transfer is critical to the subject's health and he or she is unable to give consent;

5.4.2.3the data is transferred to a corporation in which the owner of the Israeli-based database has a controlling interest (i.e. over 50 per cent) and the corporation has undertaken to maintain the privacy of the data;

5.4.2.4the transferee 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;

5.4.2.5the data has been lawfully publicised;

5.4.2.6transfer of data is necessary for the benefit or the security of the public;

5.4.2.7transfer of data is required under Israeli law; or

5.4.2.8the 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 European Union Member countries under the same terms and conditions; and (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 (as of the date indicated on the release line below, no such understandings have been reached).

As discussed above, ``consent" means informed consent, which may be express or implied.

The single exception to the general prohibition on the transfer of data is when transferring data pursuant to the Interstate Legal Assistance Law 1998, which provides for data disclosure procedures between Israel and applicable countries regarding legal proceedings.

Furthermore, an application to register a database must give details regarding the transfer of data outside the borders of the state (s.9(b)(4)). Also, a notice to a person to provide data must state to whom the information will be delivered and for what purpose (s.11).

5.5Disclosure of data by processing bureaux

As stated above, the Privacy Law does not contain a concept that is exactly equivalent to a processing bureau. However, if a particular entity carrying on a processing bureau falls within one of the categories of regulated entity, it will be subject to the relevant provisions of the Privacy Law. For instance, a processing bureau is likely to come within the definition of a ``holder" and will therefore be subject, inter alia, to the requirements set out at 5.3 above.

6 RIGHTS OF DATA SUBJECTS

6.1 Access to data held

6.1.1 General right to inspect data

Section 13(a) provides that every individual may inspect any information about him that is kept in a database, whether in person, by a representative who has written authorisation, or by a guardian (e.g. in the case of minors). The owner of the database must enable inspection of the information in Hebrew, Arabic or English, as requested (s.13(b)).

An owner of a database who employs a third party to maintain it ("the holder") 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 allow the inspection. If the applicant applied first to the holder, then the holder must inform the applicant whether he holds information about the applicant and provide the database owner's name and address (s.13A).

A form that may be used for the request is provided by the regulations issued pursuant to the Privacy Law (reg.1 of the Protection of Privacy Regulations (Conditions for Inspection of Data and Procedures for Appeal against Refusal of Request to Inspect) 1981 ("the Data Inspection Regulations")). Pursuant to reg.6 of the Data Inspection Regulations, the applicant must pay the owner or holder of the database a fee of NIS 20 for the inspection. Inspection must be permitted within 30 days of the request, although the Registrar may extend the period by an additional 15 days (reg.2(a) of the Data Inspection Regulations).

The Data Inspection Regulations allow the database owner to provide a print-out of the requested information as the equivalent of permitting inspection of the data (reg.2(b) of the Data Inspection Regulations). However, reg.3(4) of the Data Inspection Regulations provides that the person viewing the print-out cannot remove it from the premises of the database owner or holder without permission. These regulations do not expressly require the database owner to provide a print-out. It is interesting to consider how these regulations would fare if tested in court, in light of the decision by the Supreme Court that the Companies Registrar, who is obliged by the Companies Ordinance to allow public inspection of certain information which is only maintained on computers, did not fulfil his obligation merely by allowing inspection on a computer screen, but instead was obliged to provide a print-out of the information so that the recipient would have written proof of the information and the date that it was received. See BGZ 2303/90 *Eli Filipovitz v Ministry of Justice, Registrar of Companies* (1990) 46 (i) PD 410.

In 2010 the Registrar of Databases published Directive 1-2010 which imposes guidelines for identity verification methods to be used when enabling remote access by a data subject to the data subject's personal data stored in a database. See Section 3.11.3 above.

A database owner or holder may refuse the request for inspection if:

6.1.1.1 one of the provisions of s.13(e) applies to the data (see 6.1.3 below); or

6.1.1.2the 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. See reg.4 of the Data Inspection Regulations. If

the owner or holder 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) (reg.5 of the Data Inspection Regulations).

In the event the request is denied, the individual requesting the data may file a suit against the database owner in accordance with the procedures set forth in the Data Inspection Regulations.

6.1.2Exemptions from right to inspect

The Privacy Law sets out two instances in which the database owner does not have to enable the applicant to inspect the data:

6.1.2.1The owner of a database may refrain from delivering to the applicant data regarding the applicant's physical or mental health if 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 (s.13(c)).

6.1.2.2The owner of a database is not obligated to deliver data in breach of its privileged status, as prescribed under any enactment, unless the applicant is the person for whose benefit the privilege is enacted (s.13(d)). Such privileges include the privilege not to deliver information that otherwise must be disclosed as evidence, including information held by attorneys, physicians, psychologists, or social workers (see Evidence Ordinance (new version) 1971, ss.48 to 51).

6.1.3Databases not subject to right of inspection

The right to inspect data is not applicable to certain databases and certain data as follows:

6.1.3.1a database of a security authority (i.e. the police, the intelligence branch of the General Staff of the Israel Defence Forces, the military police, the General Security Service, and the Institute of Intelligence and Special Assignments);

6.1.3.2the prison service database;

6.1.3.3a tax authority's database;

6.1.3.4data as to which the security of the state, its foreign relations or the provisions of any enactment require that the data not be disclosed;

6.1.3.5databases 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 requests to inspect data about himself stored in such a database is entitled to examine any information that is not "secret information" (s.13(e)(4)). See also the Protection of Privacy Regulations (Determination of Databases Containing Non-Disclosable Data) 1987; and

6.1.3.6 the database established by the Minister of Justice, in accordance with s.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 therein), 2002.

6.2 Information about data held

There are no obligations to provide information to the data subject except in accordance with a request to inspect data (see 6.1 above), or a request to provide data (see 3.12 above).

6.3 Rectification of inaccurate data

Section 14(a) of the Privacy Law provides that if any individual inspects information about himself and finds that it is inaccurate, incomplete, unclear or not up-to-date, the person may request that the database owner or (if that owner is a foreign resident) its 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 (s.14(b) of the Privacy Law, and reg.7(a) of the Data Inspection Regulations). If the database owner refuses the request, 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) (s.14(c) of the Privacy Law and reg.17(b) of the Data Inspection Regulations). 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 (s.14(d) of the Privacy Law).

6.4 Erasure of data

There are no provisions in the Privacy Law or regulations regarding erasure of data in databases generally. However, every person (including a legal entity) may demand in writing from the owner of a database used for direct mail that the information about him be deleted from the database (s.17F(b)).

6.5 Blocking of data

There are no provisions regarding blocking of data in databases generally. However, every person (including a legal entity) 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 period of time or indefinitely (s.17F(c)).

6.6 Compensation for inaccurate data, etc.

There are no provisions specifically setting out rights to compensation for damage suffered as a result of inaccurate data. However, breaches of the Privacy Law, whether by act or omission, constitute a civil wrong under the Civil Wrongs Ordinance (new version) (ss.4 and 31B of the Privacy Law). Therefore, compensation for inaccurate data could be awarded if damage were suffered as a result of inaccurate data, provided the damage also resulted from a breach of the Privacy Law.

In addition, a civil suit can be brought for compensation for damage suffered as a result of an unauthorised disclosure of data, if the disclosure constitutes an infringement of privacy under s.2 (s.4 of the Privacy Law and 8 below).

6.7 Objection to processing

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 (see 8 below).

6.8 Other relevant rights

The Privacy Law contains no other relevant rights.

7 THE REGULATORY BODY

7.1 The regulatory body

The Registrar of Databases is appointed by the government pursuant to the Privacy Law which, together with the Registrar of Credit Details Service and the Registrar of Approving Entities (appointed pursuant to the Electronic Signature Law 2001) form the Israeli Law, Information and Technology Authority ("ILITA").

7.2 Duties and powers of the regulatory body

The Registrar is required to maintain the Registry of Databases, and is empowered to supervise compliance with provisions of the Privacy Law and the regulations issued thereunder (ss.7 and 10(c)).

The Registrar is authorised to refuse to register a database if she has reasonable grounds to assume that:

7.2.1the database is used or is liable to be used for illegal activities or as a cover for them; or

7.2.2the data included in the database were obtained, accrued or collected in breach of the Privacy Law or in breach of the provisions of any enactment (s.10(a)(1)).

This authority to refuse registration was expanded to include the second ground following a Supreme Court decision upholding the refusal of the Registrar to register a database containing information on dishonoured cheques that were to be gathered in breach of the privacy rights of those whose cheques were dishonoured. See *Registrar of Databases v Moshe Ventura* (1988) 48 (iii) PD 808.

The Registrar is also the head of a unit set up by the Minister of Justice to supervise databases, their registration and the security of the data, and the Registrar is authorised to appoint inspectors (ss.10(d) and 10(e)). The inspectors are granted broad powers under the Privacy Law. The inspectors may demand that a person furnish information and documents related to a database. Also, to ensure implementation of the Privacy Law and to prevent breaches, inspectors may enter, search and seize objects from any place at which they have a reasonable belief that a database is being operated (except that entry into a residence requires a court order) (s.10(f)).

Pursuant to s.10A of the Privacy Law, the Registrar of Databases is required to prepare an annual report about its enforcement and supervision activities during the preceding year for submission to the Constitution, Law and Justice Committee of the Parliament. The most recent report, the 2008 annual report, describes events that occurred during 2008. The report states that almost 500 databases were registered during 2008.

The annual report contains the following: (1) a discussion of the primary issues tackled by the Israeli Law, Information and Technology Authority in 2008. These included the drafting of various proposed amendments to the Privacy Law on the basis of the recommendations of the Schoffman Committee; these proposed amendments relate to the grant of additional enforcement authorities to the Registrar of Databases, a limitation of the database registration requirements and the Registrar of Companies database. The Authority also worked on the development of a twinning plan with respect to protection of personal data with the European Union. (2) a description of enforcement and supervision activities during 2008. These activities include, amongst others, supervision of (i) governmental authorities, such as the Ministry of Defence and use of the national voter's card by political parties; and (ii) inspection of complaints brought to the attention of the Registrar of Databases with respect to unauthorized use of information published in private and governmental databases by private companies. In connection with such supervision activities, the Registrar confirmed its intention to use its authority to issue administrative fines.

7.3Role of codes of practice

The Privacy Law does not provide for any codes of practice. The Registrar of Databases has issued guidelines with respect to certain activities. These guidelines do not have the status of binding law; they do however reflect the manner in which the Registrar of Databases interprets existing law.

7.4 Role of courts and tribunals

There is no special tribunal set up to handle matters relating to data protection. See 8 below with respect to the role of the courts.

7.5 Role of other organisations

The Privacy Protection Council ("the Council") was established by the Minister of Justice in order to advise the Minister of Justice on matters related to the Privacy Law, as well as to provide guidance to the Registrar of Databases. The Council may be contacted as follows:

Address: Privacy Protection Council Ministry of Justice

P.O. Box 7360

The Government Offices

125 Begin Street, Tel Aviv

Israel 61092

privacy.council@justice.gov.il

Name: Yoram Hacoheh, Adv

Title: Registrar of Databases

Address: Ministry of Justice

P.O. Box 7360

The Government Offices

125 Begin Street

Tel Aviv

Israel 61072

Tel: +972 3 7634 050

Fax: +972 2 6467 064

8 OFFENCES AND ENFORCEMENT

8.1 Summary of offences

8.1.1 Offences for infringement of privacy

An infringement of privacy is actionable as a civil wrong pursuant to s.4. A person who wilfully infringes the privacy of another in one of the ways described in ss.2(7), 2(9), 2(10) or 2(11) could, inter alia, be subject to five years' imprisonment pursuant to s.5. However, s.6 of the Privacy Law also provides that: ``No right to bring a civil or criminal action under this Law shall accrue for an infringement that has no real significance".

Section 29A provides that the court may award damages amounting to NIS 50,000 without proof of damages pursuant to ss.4 and 5. The section further stipulates that the damages may be doubled in civil wrong pursuant to s.4 upon evidence that the privacy infringement was with intent to harm.

8.1.2 Offences specifically involving databases

In addition to the civil or criminal proceedings for an infringement of privacy, the Privacy Law also contains specific offences regarding databases.

Section 16 provides that 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.

A person may be subjected to one year's imprisonment for breach of the following obligations regarding databases (s.31A(a)):

8.1.2.1 managing, possessing or using a database in breach of s.8 (i.e. the obligations to register certain databases);

8.1.2.2 delivering false details in an application for registration of a database, as required by s.9;

8.1.2.3 failing to deliver details or delivering false details in a notice attached to a request for information under s.11;

8.1.2.4 failing to comply with the provisions of ss.13 and 13A regarding the right to inspect information kept in a database, or failing to amend a database in accordance with the requirements of s.14;

8.1.2.5 granting access to a database in breach of s.17A(a), or failing to deliver documents or an affidavit to the Registrar in accordance with the provisions of s.17A(b);

8.1.2.6 failing to appoint a security officer for data security as required by s.17B;

8.1.2.7 managing or possessing a database used for direct mail services in breach of the provisions of ss.17D to 17F; and

8.1.2.8 delivering information in breach of ss.23B to 23E (regarding public bodies).

These are strict liability offences, as neither criminal intent nor negligence need be proven (s.31A(b)).

In addition to providing that an infringement of privacy is actionable as a civil wrong, s.31B of 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. See Explanatory Notes to Proposed Law, Reshumot, Hatza'at Hok 2234 (1994) at page 148.

8.1.3 Defences, exemptions and mitigating circumstances

The Privacy Law sets out a number of defences, exemptions and mitigating circumstances. For example, in criminal or civil proceedings for infringement of privacy, it is a good defence if the infringement was committed in good faith:

8.1.3.1 by someone who neither knew, nor should have known, of the possibility of an infringement of privacy;

8.1.3.2 in circumstances in which the infringer was under a legal, moral, social or professional obligation to commit the infringement, unless the infringer breached the professional ethical code or custom and provided that the infringer was not under a legal obligation to commit the infringement; and

8.1.3.3 in defence of a legitimate personal interest of the infringer (s.18(2)).

It is also a good defence if, in the circumstances, the infringement was justified by a public interest, provided that if the infringement involved a publication the publication was not untruthful (s.18(3)).

An exemption under s.19(a) provides that no person shall be responsible under the Privacy

Law for an act which he or she is empowered to do by law. This provision broadly encompasses any disclosure of data that is authorised under any statute, ordinance, or regulation. Another exemption (under s.19(b)) provides that no security authority, or person employed by it or acting on its behalf, shall be responsible under the Privacy Law for an infringement reasonably committed within the scope of their functions.

Mitigating circumstances that a court may take into account in sentencing or awarding compensation include the fact that the accused or defendant did not intend to commit an infringement (s.22).

8.2 Remedies and sanctions available

8.2.1 Criminal and civil remedies and sanctions

Criminal and/or civil proceedings may be brought based on an infringement of privacy under the Privacy Law (see 8.1 above). Criminal sanctions include fines or jail terms, and civil remedies include injunctive relief and/or monetary compensation. Details regarding fines are described in the Administrative Offense Regulations (Administrative Fine—Protection of Privacy) 2004. The Registrar of Databases has issued administrative fines e.g. in 2008 the Registrar of Databases issued administrative fines to the Municipality of Ramat Gan and a private company for unauthorised use of information included in the Ramat Gan Municipality Database.

An infringement of privacy is actionable as a civil wrong pursuant to s.4. In addition, Section 29A provides that the court may award damages amounting to NIS 50,000 without proof of damages pursuant to ss.4 and 5. The section further stipulates that the damages for civil wrongs may be doubled pursuant to s.4 upon evidence that the privacy infringement was with intent to harm.

8.3 Administrative remedies

Pursuant to s.10(f), the Registrar may apply to the District Court for an order cancelling the registration of a database or suspending the registration's validity for a specific period if:

8.3.1 the owner or holder in respect of a database infringes any provision of the Privacy Law or its regulations; or

8.3.2 the owner or holder in respect of a database fails to comply with any demand made of him or her by the Registrar.

Provided that prior to such suspension or cancellation, the owner of the database received an opportunity to make a claim against such decision.

In August 2008, the Ministry of Justice announced that for the first time, the Registrar of

Databases decided to remove two databases from the Register of Databases on the grounds that the database holder violated the provisions of the Privacy Law.

8.4 Rights of appeal

Apart from the standard rights of appeal under Israeli law from any civil or criminal proceeding, there are two specific rights of appeal granted by the Privacy Law.

Database owners may appeal to the District Court within 30 days after being served notice of certain decisions of the Registrar (such as an order by the Registrar to register a database that is otherwise exempt from registration, or a refusal by the Registrar to register a database) (ss.8(e) and 10(b)).

An individual who requests to inspect data in a database and is refused, or who receives notice from a database owner that the request to amend or delete data was rejected, is entitled to appeal to the Magistrates' Court (s.15).

9 INTERNATIONAL ASPECTS AND THE FUTURE

9.1 Council of Europe Convention

See s.4 above (reg.2(h)(i)).

9.2 European Union Directive: applicability and implementation status

In January 2011, pursuant to Directive 95/46/EC of the European Parliament, 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 Art.25 of Directive 95/46/EC. The decision extends to international automated data transfers, as well as non-automated transfers that are subject to further automated processing in Israel. The decision does not extend to international data transfers where the transfer itself, as well as the subsequent data processing, is carried out exclusively through non-automated means.

9.3 Brief summary of draft implementation legislation

Previous reports of the Registrar of Databases outlined problems and trends in connection with enforcement of the Privacy Law, and concluded that the Privacy Law has proven to be inadequate in dealing with the possibilities of infringement of individual privacy through the use of data networks and broadband data transfer from remote servers. This, together with the understanding that since the last comprehensive amendment of 1996, many technical developments have been introduced which are not addressed by the current provisions of the Privacy Law, it was made clear that a full reappraisal and assessment of data protection legislation in Israel is required, and in 2004 the Ministry of Justice appointed a Committee for the Review of the Legislation in the Field of Data Protection, which is often referred to as "Schoffman Committee". The Schoffman Committee report was published in January 2007, and included recommendations for amendment of the Privacy law.

The recommendations of the Schoffman Report, include, among others, the following:

9.3.1 Broadening this definition of "databases" to include non-computerised databases. The Report suggested the following definition: "A collection of personal data where the information can be tracked by a certain characterization or profile."

9.3.2 Replacing the existing definition of "data" with the following definition: "any details regarding an identified person or a person who can be identifiable by reasonable measures". In addition, the report proposed the cancellation of the

definition of "sensitive data" and proposed guidelines for types of data that would require registration in the Database Registrar.

9.3.3 Limiting the obligation to register a Database to the following circumstances: (a) the database owner "trades" in the information; or (b) the Database includes sensitive data. In addition, the committee recommends broadening the authority of the Registrar of Databases to require an exempt database to register, and provide the Minister of Justice with the authority to compel or exempt from registration certain types of databases.

9.3.4 Providing the Registrar of Databases with the following authorities: (a) independent discretionary power, including authority to take part in a legal proceeding of public concern; (b) setting guidelines with respect to Chapter Two of the Privacy Law; (c) the authority to issue protection of data orders. We note that a proposed amendment to the Privacy Law that would vest the Registrar with additional powers and enforcement authority was published in February 2010, but has not yet been passed into law.

9.3.5 Amending the Class Action Law to allow class actions for violations of the Privacy Law.

9.3.6 With respect to section 2(9) of the Privacy Law, which restricts the transfer and usage by a third party of information regarding individuals' private affairs other than for the purpose for which it was given, the Report recommended broadening this restriction to a wide range of personal data.

9.3.7 Requiring databases holder to introduce data security measures that will guarantee reasonable protection on the intactness of the data, its availability and confidentiality, and will prevent unauthorised use of the data, including inspecting, copying or changing the data.

9.3.8 Clarifying that the rights to inspect and amend the data (ss.13 and 14) apply only to active databases, and that the inspection rights will include that right to receive information about the type of personal data stored in the database, the sources of information of the database, whether the data is provided to third parties, and if so, the identity of such third parties and the purposes for which the data is transferred.

9.3.9 Amending the Privacy Law so that the sections regarding Direct Mail Services would apply only in those cases where the Communication Law (which contains comprehensive legislation regarding the transmission of electronic messages, such as emails, SMSs and the like) does not apply.

9.3.10 Reassessing the existing Data Transfer Regulations. In addition, it recommends that the transfer of data outside the State of Israel not in compliance with the Data Transfer Regulations constitute a criminal offence.

In addition, two sets of draft guidelines have been released by ILITA. These guidelines remain open to public comment and further revision by ILITA, after which they will be re-released in final form.

In December 2010, ILITA published draft ethical and behavioural guidelines for database owners collecting data from minors. 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:

- (1) A general obligation to employ privacy by design principles (i.e., designing privacy and data protection compliance into data systems from the start) in a manner designed to protect minors and minimize the risk to their privacy.
- (2) 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.
- (3) 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.
- (4) 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.
- (5) Obliging suppliers who collect data concerning minors to draft a “privacy policy” and a clear abstract of this document.
- (6) Prohibition on the publication of data which enables the identification of a child minor under the age of 14.
- (7) Deletion of data once it is no longer necessary or at the request of the minor or parent.
- (8) Allowing the database owner to prove compliance with the said principles by examination of an independent auditor.

In addition, in January 2011 ILITA published draft guidelines applicable to the collection and use of personal data provided by job applicants to companies providing pre-employment evaluation and screening services (“Placement Institutes”) and to the

test results generated by such entities, which guidelines address the following, among other matters:

(1) For purposes of the Privacy Law, the Placement Institute acts solely as a “holder” of applicants’ personal data, while the potential employer is the “owner” of such data.

(2) Any use of data by the potential employer other than for purposes of evaluating the applicant’s candidacy for employment requires express data subject consent.

(3) Consent alone is not sufficient to support any and all use of applicant data; use of applicant data must also meet the legitimate business purpose and proportionality tests; i.e., such data may be used only for a legitimate business purpose, the information must be relevant to the achievement of such legitimate purpose, such purpose must not be achievable by means other than collection of the information, and the benefits derived from retention and processing of personal information must exceed the attendant invasion of the applicant’s privacy.

(4) Placement Institutes and prospective employers must allow applicants undergoing evaluations to receive test scores, results and reports transmitted to employers in the form in which they are received by employers (other than data exempt from disclosure pursuant to Section 13 of the Privacy Law and test questions or other Placement Institute trade secrets). Such results must be provided within thirty days, without charge. Applicants must receive notice of the right to receive this information prior to their consenting to the collection of data.

(5) The Placement Institute and the employer must destroy or fully anonymize applicant data once evaluation activities have been completed.

(6) The Guidelines acknowledge that under the Privacy Law, “consent” means informed consent, which may be express or implied, and that the job applicant’s provision of information to a prospective employer or Placement Agency after receiving appropriate explanations regarding the purpose for which the information will be used can be sufficient evidence of the applicant’s implied consent to the use of the information for the stated purpose. However, it is preferable that applicants’ express consent be obtained for the use of information provided to employers. In addition, where particularly sensitive information is collected, express consent would be required. The Guidelines also note that information requested from job applicants and the tests to which they are subjected must be consistent with proportionality and proper purpose principles.

ANNEX LIST OF PRIMARY AND SECONDARY LEGISLATION

<i>Primary legislation</i>	<i>Number</i>	<i>Date in force</i>
Protection of Privacy Law 1981	1011	
Chapter Two of the Law		September 12, 1981
Remainder of the Law		March 11, 1981
Amendment to Protection of Privacy Law 1981	1016	April 7, 1981
Amendment to Protection of Privacy Law 1985	1137	March 7, 1985
Amendment to Protection of Privacy Law 1995	1497	December 28, 1995
Amendment to Protection of Privacy Law 1995 (No. 2)	1526	June 9, 1995
Amendment to Protection of Privacy Law 1996	1589	
Sections 17A and 17B		October 12, 1996
Sections 17C–17I		April 12, 1997
Section 10A		April 1, 1997
Remainder of the Amendment		April 11, 1997
Amendment to Protection of Privacy Law 1981	1625	December 3, 1996
Amendment to Protection of Privacy Law 1981	1753	July 2, 2000
Amendment to Protection of Privacy Law 1981	2020	August 8, 2005
Amendment to Protection of Privacy Law 1981	2038	December 8, 2005
Amendment to Protection of Privacy Law 1981 (No. 9)	2101	June 26, 2007
Amendment to Protection of Privacy Law 1981	2198	November 16, 2008
Credit Reporting Law 2002		February 1, 2003
<i>Secondary legislation</i>	<i>Number</i>	<i>Date in force</i>
Protection of Privacy Regulations (Determination of Databases Containing Non-Disclosable Data) 1986	5022	March 1, 1987
Amendment 2005	6422	December 19, 2005
Protection of Privacy Regulations (Conditions for Possessing and Protecting Data and Procedures for Transferring Data Between Public Bodies) 1987	4931	February 12, 1987
Protection of Privacy Regulations (Conditions for Inspection of Data and Procedures for Appeal from a Refusal of a Denial of a Request to Inspect) 1981	4270	September
	4794	11, 1981
	6193	April 18,

Amendment 1985		1985
Amendment 2002		August 26, 2002
Protection of Privacy Regulations (Fees) 2000	6069	January 1, 2001
Last amended: 2009	6843	December 29, 2009
Administrative Offences Regulations (Administrative Fine—Protection of Privacy) 2004	6299	April 26, 2004
Protection of Privacy Regulations (Transfer of Information to Databases outside of the State's Boundaries) 2001	6116	January 2, 2002
Protection of Privacy Order (Determination of Public Bodies) 1986	4898	February 2, 1986
Last amended: 2006	6476	April 23, 2006