ISRAEL

Last modified 28 January 2019

LAW

The laws that govern the right to privacy in Israel are the Basic Law: Human Dignity and Liberty, 5752 - 1992; the Protection of Privacy Law, 5741-1981 and the regulations promulgated thereunder (the PPL); and the guidelines of the Israel Privacy Protection Authority.

DEFINITIONS

Definition of Personal Data

Personal data, as defined under the PPL, means: data regarding the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.

Definition of Sensitive Personal Data

Sensitive data, as defined under the PPL, means: data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person; and other information if designated as such by the Minister of Justice with the approval of the Constitution, Law and Justice Committee of the Knesset. No such determination has been made to date.

NATIONAL DATA PROTECTION AUTHORITY

The Israel Privacy Protection Authority (PPA), established in September 2006, as determined by Israel’s Government decision no. 4660, dated January 19, 2006.

REGISTRATION

Subject to certain exceptions, database registration is required to the extent one of the following conditions are met:

- The database contains information in respect of more than 10,000 data subjects
- The database contains sensitive information
- The database includes information on persons, and the information was not provided by them, on their behalf or with their consent
- The database belongs to a public entity
- The database is used for direct-marketing services

Subject to certain exceptions, a database is defined under the PPL as a collection of data, stored by magnetic or optic means and intended for computer processing, consequently excluding non-computerized collections.
In 2005, the Ministry of Justice set up a committee generally known as the ‘Schoffman Committee’ which recommended relaxing registration of ordinary databases and focusing on specific categories of information (e.g., medical data, criminal records or information about a person’s political or religious beliefs). However, to date, the Schoffman Committee recommendations have not crystallized into binding legislation.

On November 28, 2018, the IPA published a statement of opinion regarding collection of email addresses. The statement asserts that the provisions applicable to databases under the PPL also would apply to a computerized list containing a collection of email addresses alongside their owners’ names.

### DATA PROTECTION OFFICERS

Appointment of a Data Protection Officer is required by an entity meeting one of the following conditions:

- Possessing five databases that require registration
- Being a public body as defined in section 23 to the POPL
- Being a bank, insurance company or a company engaging in rating or evaluating credit

Failure to nominate a Data Protection Officer when required to do so may result in criminal sanctions, including administrative fines. The PPL does not require that the Data Protection Officer be an Israeli citizen or resident.

If a company appoints a data protection officer pursuant to the PPL, then Israel Protection of Privacy Regulations (Data Security), 5777-2017 (Data Security Regulations) require that the officer be directly subordinate to the database manager, or to the manager of the entity that owns or holds the database. In addition, the Data Security Regulations prohibit the officer from being in a conflict of interest and require the officer to establish data security protocols and ongoing plans to review compliance with the Data Security Regulations. The officer must present findings from such review to the database manager and its supervisor.

### COLLECTION & PROCESSING

The collection, processing or use of personal data is permitted subject to obtaining the informed consent of the data subjects. Such consent should adhere to purpose, proportionality and transparency limitations. As such, consent should be obtained for specific purposes of use, the processing and use of personal data should be proportionate to those purposes, and data subjects should have the right to inspect and correct their personal data. The data subject’s consent must be re-obtained for any change in the purpose of use.

Any request for consent from a data subject to have his or her personal data stored and used within a database must be accompanied by a notice indicating:

- Whether there is a legal requirement to provide the information
- The purpose for which the information is requested
- The recipients of the data, and
- The purpose(s) of use of the data

Retaining outsourcing services for the processing of personal data is subject to the PPA’s Guidelines on the Use of Outsourcing Services of Processing Personal Information (Guideline 2 2011) dated June 10, 2012 (Outsourcing Guidelines). The Outsourcing Guidelines include, inter alia, factors to be taken into consideration when deciding to use outsourcing services, specific provisions to be included within the data transfer agreement, and data security requirements. Processing of personal data in certain sectors is subject to additional outsourcing requirements.

The Outsourcing Guidelines require compliance with the Data Security Regulations.

Entities subject to separate outsourcing guidelines are, for example, entities supervised by the Commissioner of the Capital
Market, Insurance and Savings, and entities supervised by the Banking Supervision Department of the Bank of Israel. On February 27, 2018, the PPA published draft guidelines regarding the applicability of the Data Security Regulations to managing companies and insurers supervised by the Israel Capital Market, Insurance and Savings Authority. The draft guidelines state that supervised organizations that are subject to and comply with the Israel Capital Market, Insurance and Savings Authority information security directives will be deemed compliant with the Data Security Regulations upon meeting specific conditions set forth in the draft guidelines. On September 10, 2014, the Banking Supervision Department of the Bank of Israel issued draft guidelines regarding risk management in cloud computing services used by Israeli banking corporations. The guidelines were recently revised (November 13, 2018) to revoke the obligation on supervised entities to receive the approval of the Supervisor of Banks prior to using cloud computing services. However, the Supervisor of Banks has not lifted the ban on using cloud computing services for core activities and core systems.

The general issue of privacy consideration in the use of surveillance cameras is governed by the IPA Use of Security and Surveillance Cameras and the Footage Obtained Therein Guidelines (no. 4/2012, dated October 21, 2012). The IPA published additional supplementary Guidelines (no. 5/17, dated October 17, 2017), specifically referring to the use of surveillance cameras in the workplace. The draft guidelines state that the employer’s prerogative to use surveillance means in the workplace is subject to the fulfillment of principals such as legitimacy, transparency, proportionality, good faith and fairness. These principles also apply to businesses required by law enforcement to place surveillance cameras on their premises. The guidelines specify the manner in which these principles should be implemented, derivative requirements and possible implications. Recently (July 5, 2018), the PPA published its position specifically addressing the use of surveillance cameras in kindergartens. The PPA position provides that an organization must seek legal advice and conduct a comprehensive examination of whether the installation of cameras is necessary to the protection of children, and whether the resulted infringement of privacy will not exceed the potential benefit from such installation.

TRANSFER

The transfer of personal data abroad is subject to the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761-2001, pursuant to which personal data may be transferred abroad only to the extent that:

- The laws of the country to which the data is transferred ensure a level of protection, no lesser than the level of protection of data provided for by Israeli Law, or

- One of the following conditions is met:
  - The data subject has consented to the transfer
  - The consent of the data subject cannot be obtained and the transfer is vital to the protection of his or her health or physical well-being
  - The data is transferred to a corporation under the control of the owner of the database from which the data is transferred, provided that such corporation has guaranteed the protection of privacy after the transfer
  - The data is transferred to an entity bound by an agreement with the database owner, to comply with the conditions governing the use of the data as applicable under Israeli Laws, mutatis mutandis
  - Data was made available to the public or was opened for public inspection by legal authority
  - Transfer of data is vital to public safety or security
  - The transfer of data is required by Israeli Law
  - Data is transferred to a database in a country:
    - Which is a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data, or
    - Which receives data from Member States of the European Community, under the same terms of
acceptance, or

- In relation to which the Registrar of Databases announced, in an announcement published in the Official Gazette (Reshumot), that it has an authority for the protection of privacy, after reaching an arrangement for cooperation with that authority.

When transferring personal data abroad, the database owner is required to enter into a data transfer agreement with the data recipient, pursuant to which the recipient undertakes to apply adequate measures to ensure the privacy of the data subjects and guarantees that the data shall not be further transferred to any third party.

The foregoing data transfer agreement must also comply with additional restrictions, to the extent that the recipient provides outsourcing services, as set forth in the Outsourcing Guidelines.

On January 31, 2011, the European Commission, on the basis of Article 25(6) of directive 95/46/EC, determined that the State of Israel ensures an adequate level of protection with regard to automated processing of personal data.

Additionally, the transfer of databases is subject to the IPA Draft Guidelines No. 3/2017 dated August 13, 2017, regarding the interpretation and implementation of the provisions of the PPL further to transfer of ownership of databases and its implications on data subject rights, which under certain circumstances, such as database recipient having a conflict of interest, might require opt-in consents from data subjects as a condition to transferring databases.

SECURITY

On March 21, 2017, the Constitution, Law, and Justice Committee of the Knesset approved the Data Security Regulations, which came into effect in May 2018. The Data Security Regulations specify the manner in which the general information security requirements under the PPL are to be implemented. The Data Security Regulations further broaden the PPL by imposing additional requirements applicable to database owners (controllers), holders (processors) and managers. Such additional requirements include, without limitation, the creation and implementation of a broad list of manuals, policies, practices and documents, such as: Database Definitions Document; Data Security Protocol; Database Mapping Document; Database Inventory; Valid Authorization List (including all authorized access personnel, titles, and database access level); Mobile Device Policy; Backup Policy and Recovery Procedure Document; and others; various physical, environmental and logical security measures; and regular audit, inspection and training obligations. The requirements under the Data Security Regulations are categorized in accordance with the level of sensitivity (high / medium / low) of the database.

The Data Security Regulations add to the Outsourcing Guidelines, which in effect expand the requirements applicable when outsourcing processing services, even prior to entering into a data transfer agreement between the database owner and the data recipient and the requirements to be included therein.

Failure to comply with the Data Security Regulations will constitute a breach of the PPL, which may expose a noncompliant entity to criminal and civil liability, as well as to administrative fines.

On September 2, 2018, the IPA published, by virtue of its cross-supervision authority, audit questionnaires in respect of personal information managed or maintained in databases. Organizations that manage or maintain such information are required to answer the questionnaires for the purpose of assessing their compliance with the provisions of the PPL and regulations promulgated thereunder, inter alia, regarding the manner of obtaining data subjects consent to use the information, the types of use of such information and the processing and security measures taken with respect thereof.

BREACH NOTIFICATION

Pursuant to the Data Security Regulations, data breach notifications are required depending on the severity of the breach and the level of security of the database. Such notifications are generally provided to the IPA which may require further notification to the data subjects.

Along with the publication of the Data Security Regulations, the PPA published its policy regarding the applicable notification obligations pursuant to a data breach and the IPA’s discretion in enforcement of such obligations.
ENFORCEMENT

PPA has the authority and obligation to supervise compliance and enforce the provisions of the PPL and appoint inspectors to carry out those activities.

Breach of the PPL may result in both civil and criminal sanctions, including administrative fines, one to five years of imprisonment and the right to receive statutory damages under civil proceedings without the need to prove actual damages.

On January 21, 2018, the Israeli Ministerial Committee for Legislation approved a draft bill for the 13th Amendment of the PPL for broadening the PPA’s enforcement powers. The current draft bill provides IPA with the ability to conduct criminal investigations and to impose monetary sanctions in the amount of up to 3.2 million. The draft bill passed its first reading in the Knesset in March 2018 but has yet to pass the approval of the Knesset Constitution, Law and Justice Committee; thereafter it would need to also pass the second and third readings in the Knesset, in order to become a binding piece of legislation.

ELECTRONIC MARKETING

Unsolicited marketing is regulated under the Communications Law (Telecommunications and Broadcasting), 5742-1982 (the Anti-Spam Act). The Anti-Spam Act prohibits, subject to certain exceptions, automated messaging sent electronically via email, automatic dialing system, fax or text messages, mainly for marketing and promotional purposes, without first obtaining the recipient’s initial opt-in prior consent; all such communications also must contain an opt-out or an unsubscribe option.

The PPL governs the possession and management of databases intended for direct mailing and direct mailing services. Direct mailing is defined in Section 17C of the PPL as personally contacting a person, based on his belonging to a group of the population that is determined by one or more characteristics of the data subjects listed in the database. Direct mailing services are also defined in the same Section as providing direct mailing services to others by way of transferring lists, labels or data by any means. The PPL imposes restrictions in connection therewith, including without limitation: mandatory notification requirements in respect of the registered database number; the identity and contact details of the respective database owner; the source of the data; database registration requirement (regardless of the number of data subjects listed or the sensitivity of the data), specifying the purpose of direct mailing; specific record-keeping requirements; compliance with data subjects’ rights of access, rectification and deletion of data from the database or banning its onward transfer.

The IPA Guidelines No. 2/2017 for the interpretation and implementation of the PPL provisions with respect of direct mail and direct mail services, intends to clarify these additional restrictions and stricter regulations with respect of direct mailing and direct mailing services. Additionally, the said IPA Guidelines govern direct marketing services which, inter alia, require specific opt-in consents and notice requirements.

ONLINE PRIVACY

The PPL does not specifically address online privacy, cookies and / or location data, all of which are governed by the general restrictions detailed above, including the requirements imposed on processing databases, direct marketing and the consent, purpose and proportionality restrictions.

The PPL governs information "about a person." As such, depending upon the circumstances at hand, any non-identifiable and anonymous information (which cannot be re-identified) may reasonably be interpreted as falling outside the confines of the PPL limitations.
KEY CONTACTS

Goldfarb Seligman & Co., Law Offices
www.goldfarb.com

Sharon Aloni
Partner
T +972 (3) 608 9834
sharon.aloni@goldfarb.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization’s level of data protection maturity.
Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.