ISRAEL

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 Authority (as defined below).

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 Authority (“IPA”), established in September 2006, as determined by Israel’s Government decision no. 4660, dated 19.01.2006.

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, or
- the database is used for directmarketing services.

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 noncomputerized 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 11, 2018, the IPA published Opinion: Is the Collection of Names and Emails Considered a “Database”? in which the IPA ruled that a list of emails is deemed Personal Data.

DATA PROTECTION OFFICERS

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

- a possessor of five databases that require registration
- a public body as defined in Section 23 to the PPL, or
- a bank, an 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 should be an Israeli citizen or resident.

In the event that a data protection officer was appointed pursuant to the PPL, the Israel Protection of Privacy Regulations (Data Security), 5777-2017 (‘Data Security Regs’) 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 Regs 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 Regs. 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 information. The data subject's consent must be reobtained 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 personally identifiable information is subject to the IPA’s Guidelines on the Use of Outsourcing Services of Processing Personal Information (Guideline 2 2011) dated 10 June 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 personally identifiable information in certain sectors is subject to additional outsourcing requirements.

Furthermore, the Outsourcing Guidelines also require compliance with the Data Security Regs.

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 10 September 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. Among other various restrictions, the draft guidelines set forth an obligation on supervised entities to receive the approval of the Supervisor of Banks prior to using cloud computing services.

The general issue of privacy consideration in the use of surveillance cameras is governed by the IPA Use of Surveillance Cameras and the Footage Obtained Therein Guidelines (no. 4/2012). In 2017, the IPA published Use of Surveillance Cameras in the Workplace and in Working Relationships Guidelines (no. 5/17) specifically referring to the use of surveillance cameras in the
workplace. The guidelines state that the employer’s prerogative to use surveillance means in the workplace is subject to fulfillment of principals such as legitimacy, transparency, proportionality, good faith and fairness. These principles apply also 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.

Furthermore, on December 23, 2018, the PIA published the Registrar Draft Guideline: Privacy Aspects of Use of Drones. This Draft Guideline applies to Personal Data collected through the use of drones. The Draft Guideline requires that the drone user take into account alternatives that will not violate the privacy of others and to activate the drone proportionately in order to minimize the scope of Personal Data collected, processed and stored. The period in which the Personal Data is retained shall be limited as much as possible and for as long as the Personal Data is stored on the drone, the drone is to be kept in a physically safe location.

TRANSFER

The transfer of personal data abroad is subject to the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 57612001, 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 wellbeing;
  - 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; or
  - 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\(^{[1]}\), 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, which under certain circumstances, such as database recipient having a conflict of interest, might require opt-in consents of data subjects as a condition to transferring databases.
Footnote 1: Following the decision of the ECJ in Case C362/14 Maximillian Schrems v Data Protection Commissioner, IPA issued a statement on October 15, 2015, according to which US safe harbour certified entities would not fall under the foregoing condition, without derogating from all other conditions.

SECURITY

On March 21, 2017, the Constitution, Law, and Justice Committee of the Knesset approved the Data Security Regs, which have come into effect on May 2018. The Data Security Regs further broaden the PPL by imposing additional requirements applicable to database owners, holders and managers. Such additional requirements include, without limitation, having in place a broad list of manuals and policies; various physical, environmental and logical security measures; and regular audit, inspection and training obligations.

Furthermore, the Data Security Regs add to the Outsourcing Guidelines, which in effect would 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 Regs will constitute a breach of the PPL, which may expose a non-compliant entity to criminal and civil liability, as well as to administrative fines.

In March and April of 2018, the IPA published guidelines regarding the applicability of the Data Security Regs to four types of organizations: organizations certified to ISO/IEC 27001 standard, supervised entities subject to the directives of the Supervisor of the Bank, management companies and insurers which are subject to the provisions of the Capital Market, Insurance and Savings Authority and non-bank stock exchange members subject to stock exchange regulations. These types of organizations only need to comply with selective provisions of the Data Security Regs.

On May 1, 2018, the IPA published the Privacy Protection Authority’s Policy for Reporting Severe Security Incidents. The directive sets forth the instructions on how to report a severe security incident. Failure to comply with the directive may lead to sanctions such as advertising the violation or deletion of database registration.

BREACH NOTIFICATION

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

ENFORCEMENT

IPA 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, 15 years of imprisonment, and the right to receive statutory damages under civil proceedings without the need to prove actual damages.

The current draft bill for the 12th Amendment of the PPL provides IPA with the ability to conduct criminal investigations and to impose monetary sanctions in the amount of up to NIS 3.2 million. The draft bill has passed its first reading, 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 order to become a binding piece of legislation.

ELECTRONIC MARKETING

Unsolicited marketing is regulated under the Communications Law (Telecommunications and Broadcasting), 1982 (the 'Anti Spam Act'). The Anti Spam Act prohibits, subject to certain exceptions, advertising by means of automated dialing, fax or text messages without first obtaining the recipient’s initial optin prior consent; all such communications also must contain an optout / unsubscribe option.

Furthermore, the PPL governs the possession and management of databases intended for direct mailing service and imposes
restrictions in connection therewith, including a database registration requirement specifying the purpose of direct mailing and specific recordkeeping requirements. Moreover, the IPA Guidelines No. 2/2017 impose additional requirements intended for direct mailing services, which, inter alia, include specific notice obligations such as indication of database information, sources and an initial opt-in requirement.

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 and 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 nonidentifiable and anonymous information (which cannot be reidentified) 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
Goldfarb Seligman & Co., Law Offices
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.