DATA PROTECTION LAWS OF THE WORLD

Israel

ISRAEL

Last modified 22 December 2023

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.[1]

1: On July 23, 2020, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Definitions and Limiting Registration Obligations) 5782- 2021. The draft bill proposes to revise defined terms under the PPL to align with the definition in the GDPR, such as definition of: personal data, sensitive data, processing, owner of a database, holder of a database and other. In addition, the draft bill attempts to limit database registration requirements to apply to certain categories of databases containing information of 100,000 data subject or more. The draft bill has yet to be placed on the table of the Israel Knesset for its first reading. Furthermore, the draft bill expands the administrative enforcement of the IPA. On May 18, 2021, the Israeli Ministry of Justice published two draft bills proposing to amend the PPL (Appointment of an Official Representative) 5782-2021 and the PPL (Minor's Privacy) 5782-2021. On July 26, 2021, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Limitation Period) 5721-2021 to extend the limitation period by which a civil claim may be filed under the PPL from a period of two years to a period of seven years, in accordance with the Statute of Limitations Law 5718-1958. All the foregoing draft bills have been placed on the table of the Israel Knesset and for their preliminary discussion. On January 5, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Amendment Number 14) 5782-2021. The draft bill proposes to increase the supervisory and enforcement capabilities of the IPA (such as impose financial sanctions for violating the provisions of the law concerning the management of databases up to an amount of NIS 3.2 million), to reduce the obligation to register databases as well as to adapt the defined terms under the Israel Protection of Privacy Law to the technological developments and modern privacy legislation. The draft bill has been approved in its first reading of the Israel Knesset and is in preparation for the second and third reading in the Knesset committee. On January 31, 2022, the Israeli Ministry of Justice published a draft bill proposing to

amend the PPL (Strengthening the Right to Privacy and its Protection) 5782-2021. The draft bill proposes additional rights of data subjects to control their personal information. In addition, the draft bill includes further strengthening of the enforcement powers of the IPA, in particular with regards to enforcement on an international level. The draft has been set on the Knesset's table for its first reading. On January 31, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Deletion from Databases), 5782-2022. The draft bill proposes to add requirements to the notification obligations to data subjects, prior to collecting personal information (Section 11 of PPL), such as adding an obligation to indicate when a renewed authorization to hold the personal information will be requested and deleting the personal information either by the data subject contacting the owner of the database, or automatically if five years have passed since receiving a notification, and no renewed authorization to hold the personal information was received. The draft bill has been approved in its first reading of the Israel Knesset and is awaiting the Knesset committee to appoint a handling committee.

On February 16, 2023, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL: (Prohibition on Publishing a Recording of an Individual) 5783- 2023, which proposes to prohibit publishing a recording of an individual in public which contains Sensitive Data. The draft bill has been placed on the table of the Israel Knesset and for its preliminary discussion.

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[1]:

- 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 direct marketing 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.

1: On July 23, 2020, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Definitions and Limiting Registration Obligations) 5782- 2021. The draft bill proposes to revise defined terms under the PPL to align with the definition in the GDPR, such as definition of: personal data, sensitive data, processing, owner of a database, holder of a database and other. In addition, the draft bill attempts to limit database registration requirements to apply to certain categories of databases containing information of 100,000 data subject or more. The draft bill has yet to be placed on the table of the Israel Knesset for its first reading. Furthermore, the draft bill expands the administrative enforcement of the IPA. On May 18, 2021, the Israeli Ministry of Justice published two draft bills proposing to amend the PPL (Appointment of an Official Representative) 5782-2021 and the PPL (Minor's Privacy) 5782-2021. On July 26, 2021, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Limitation Period) 5721-2021 to extend the limitation period by which a civil claim may be filed under the PPL from a period of two years to a period of seven years, in accordance with the Statute of Limitations Law 5718-1958. All the foregoing draft bills

have been placed on the table of the Israel Knesset and for their preliminary discussion. On January 5, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Amendment Number 14) 5782-2021. The draft bill proposes to increase the supervisory and enforcement capabilities of the IPA (such as impose financial sanctions for violating the provisions of the law concerning the management of databases up to an amount of NIS 3.2 million), to reduce the obligation to register databases as well as to adapt the defined terms under the Israel Protection of Privacy Law to the technological developments and modern privacy legislation. The draft bill has been approved in its first reading of the Israel Knesset and is in preparation for the second and third reading in the Knesset committee. On January 31, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Strengthening the Right to Privacy and its Protection) 5782-2021. The draft bill proposes additional rights of data subjects to control their personal information. In addition, the draft bill includes further strengthening of the enforcement powers of the IPA, in particular with regards to enforcement on an international level. The draft has been set on the Knesset's table for its first reading. On January 31, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Deletion from Databases), 5782-2022. The draft bill proposes to add requirements to the notification obligations to data subjects, prior to collecting personal information (Section 11 of PPL), such as adding an obligation to indicate when a renewed authorization to hold the personal information will be requested and deleting the personal information either by the data subject contacting the owner of the database, or automatically if five years have passed since receiving a notification, and no renewed authorization to hold the personal information was received. The draft bill has been approved in its first reading of the Israel Knesset and is awaiting the Knesset committee to appoint a handling committee.

On February 16, 2023, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL: (Prohibition on Publishing a Recording of an Individual) 5783- 2023, which proposes to prohibit publishing a recording of an individual in public which contains Sensitive Data. The draft bill has been placed on the table of the Israel Knesset and for its preliminary discussion.

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 olio, 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.

On December 27, 2018. The Camera Installation Law for the Protection of Toddlers in Day Care Centers for Toddlers (5779 - 2018) was published and became effective on September 1, 2020. The said law provides that the operator of a daycare center for toddlers is required (unless it falls under the exceptions under the law) to install cameras that will record during the time of which the toddlers are present, without sound. It is forbidden to view the videos, to copy them, to transfer them to another person and to make any use of them without a court order (except for the Police and the Ministry of Welfare officials for the purpose of preventing harm to toddlers that are in the daycare). No real-time viewing of the footage is permitted, and it must be deleted withing 30 days from the date of filming.

On July 8, 2023, the Israeli Ministry of Justice published: Amendment to Installation of Cameras for the Protection of Toddlers in Daycare Centers for Toddlers (Amendment No. 1), 5779 -2017, which intends to strike a balance between the need to protect toddlers and the need to reduce as much as possible the harm to the privacy of the toddlers and the daycare staff, usually from photographing and viewing the photographs. The draft bill has been placed on the table of the Israel Knesset and for their preliminary discussion.

On October 16, 2023, The IPA published Publication: Protecting the Privacy of Students in Distance Learning, which presents a number of emphases and recommendations for proper conduct and protection of privacy and Personal Information as part of students' use of online distance learning applications.

Furthermore, on March 29, 2020 its Recommendations: Privacy Aspects of Use of Drones which, recommends 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 should 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; ensure privacy by design and compliance with the PPA requirements in respect of privacy by notification, transparency and deletion of data.

On August 31, 2021, the IPA published Draft Guidelines: Collection of Employee Location Data Using Dedicated Apps and Vehicle Location Systems. The guidelines emphasize that such a use shall only be made in the absence of an alternative. The employer must further determine in advance the purpose, the specific range of hours Personal Data collection, and the duration for which the information will be retained.

On May 22, 2023, the IPA published Publication: Privacy Related Aspects of Monitoring Remote Working Employees, which includes certain standards required for employers that monitor their employees working remotely in order to avoid breach of their privacy rights (including without limitation compliance with proportionality and legitimacy standards such as limiting

surveillance solely to work hours; employers must inform their employees that they are using technological means to monitor their behavior when working remotely, including the purpose for which the monitoring is done).

On July 26, 2023, the IPA published Opinion: Collecting Location Data of Employees Using Applications and In-Vehicle Tracking Systems, which determines guidelines on how to collect such data from employees in their vehicles provided by the employer.

On March 25, 2021, the IPA published Policies of Data Minimization, which require database owners to: ensure that the information collected is and will be required to achieve the purpose of for which it was collected and is deleted thereafter; check annually if they possess data that is irrelevant etc.

On December 12, 2022, the IPA published Guidelines: What are ‘Data’ and ‘Information on a Person’s Private Affairs’ according to the PPL, which clarifies the meaning of the terms Data and Information on a Person's Private Affairs.

On July 23, 2020, the Special Authorities to Combat the Novel Corona Virus (Temporary Order) 5780 – 2020 came into effect (by virtue of the Israel Government's authority under Section 39 of the Basic Law: The Government). Under the Temporary Order, and the authorities granted to the Israel General Security Service ('GSS') by the General Security Service Authorization Law 5762-2002, the Government may establish new regulations which potentially broaden Israel Government authorities / GSS rights in respect of collection and processing Personal Data, such as: the Emergency Regulations (General Security Service Authorization to Assist in the National Effort to Reduce the Spread of the Novel Corona Virus), 5780- 2020 which authorized the GSS to perform surveillance on Israel citizens to reduce the spread of the Corona Virus; Emergency Regulations (Location Data), 5780-2020 were established amending the Criminal Procedure Law (Enforcement Powers – Communication Data) 5768- 2007 authorizing the Israel Police to preform cell phone surveillance (i.e. receiving the location of a cell phone from a cellular operator) of a Corona virus patient without a court order; and the Emergency Regulation (General Security Service to assist in National Effort to Reduce Spread of Omicron Strain of Novel Corona Virus), 5782- 2021 that permit the GSS to perform surveillance of Israel citizens. The Temporary Order has been extended until February 15, 2024, in order to maintain a legal infrastructure that enables taking actions under the law to reduce the spread of the coronavirus and reduce harm to public health.

On January 2022, the IPA published Recommended Guidelines: Appointment of a Privacy Protection Officer ("PPO") and its Roles and Responsibilities. In Israel, there is no obligation to appoint a PPO, but the IPA recommends appointing one in organizations that collect and process Personal Data, databases owners and holders in a database. Appointing a PPO helps the organization verifying that it complies with the provisions of the PPL and the Data Security Regs and is indication that the organization has taken and takes steps to reduce the risk of damage to the Personal Data kept in its possession. In the recommended guidelines, the IPA refers to the scope of the PPO's role, which will be determined according to the complexity of the data processing operations carried out in the organization and according to its size. Also, the roles and tasks that are recommended to be under the care of a PPO are, among others, regulation of information management processes, supervision and control and training and implementation.

On July 31, 2022, the IPA published Obligation to Notify as Part of Collection and Use of Personal Information Guideline. The guideline requires notification to data subjects which their Personal Data is collected and used by systems for making algorithm-based or artificial intelligence decisions.

On February 20, 2023, the Committee of Ministers for Legislative Affairs published Amendment to the Police Order (No. 40) (Biometric Photographic System) 5783- 2023, which regulates aspects of placing systems that capture biometric photos in public spaces by the police. The photo systems include the capabilities to process the photos of people and compare them to identifiable information entered into the system, in a way that may allow indemnification.

On June 6, 2023, Inclusion of Biometric Identification Means and Biometric Identification Data in Identification Documents and in the Database (Amendment and Temporary Order), 5777-2017, came into effect, which allows the collection of fingerprints for the police's public biometric database, until June 30, 2024.

Furthermore, On October 14, 2023, the Israeli Ministry of Justice published Emergency Regulations: IDF Authorization to Perform an Operation on Computers Used for Activating Cameras, which authorize IDF soldiers (which have required skills) to penetrate and operate on computers used to operate stationary cameras, without receiving consent of the person who owns the computer, under certain circumstances, such as: the penetration of the computer: (i) is essential for preventing access to information, which has the potential to actually endanger the security of the state or the continuity of the operational functioning of the IDF; (ii) is required immediately and urgently; or (iii) it is not possible, in the timeframe to obtain the consent of the owner of the computer.

On November 15, 2023, The IPA published publication: Privacy in Home IoT Products and Smart Homes, which includes recommendations to companies that provide IoT (Internet of Things) services and products in the home space, as part of transforming homes into "smart homes" and to such users, as the smart home devices collects and processes a large amount of Personal Data and Sensitive Data and introduction of surveillance systems into the areas of the individual's private and intimate space.

On August 22, 2023, the IPA published Publication: Disclosure of Personal Information Regarding Male and Female Students on The Websites of Higher Education Institutions, which includes guidelines as to manner of such disclosure.

On December 11, 2023, the government published Memorandum of Law: Israel Security Agency (Amendment No....), 2023 open to comments by the public, which purpose is to regulate certain aspects including cyber and computers and to grant GSS rights to receive, collect and transmit information, including from databases, subject to certain approvals, supervision and control mechanisms. Which is in addition to the publication by the Israeli Ministry of Justice published on February 28, 2021 the draft bill Memorandum: "The Cyber Defense Law and the National Cyber System (Authorities for the Purpose of Strengthening Protection) (Temporary Order), 5781-2021", which states that the National Cyber System and the GSS will be permitted to give instructions to private and public organizations in Israel on how to prepare for and defend against a cyber-attack and addresses compliance issues.

On December 29, 2022, the IPA published Recommendations for Proper Conduct When Using Applications (Apps) to Pay and Validate Public Transportation, including without limitation recommendations in respect of privacy policies, app information security, deletion of Personal Data and other.

On January 24, 2023, the Israeli Ministry of Justice published Memorandum: "Health Information Mobility Law, 5783-2023", to regulate patient's access to their health information in connection with provision of health services while protecting their privacy and data security.

On August 8, 2023 the IPA published: The Right of Inspection Regarding the Databases of Entities Listed in Section 13(e) of The PPL, which grants individuals the right of inspection in respect of the databases of the entities listed in Section 13 (e) of the PPL (such as security authorities, prison service, tax authority, Minister of Justice, and other).

TRANSFER

The transfer of Personal Data abroad is subject to the Privacy Protection Regulations (Transfer of Data to Databases Abroad), 5761-2001 ("**Transfer Regs**"), 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.

On January 4, 2022, the IPA published a Draft Guideline: Interpretation of Section 3 of Transfer Regs, clarifying the prohibition on onward transfer of Personal Data by a data recipient stipulating that where the following applies, such onward transfer may be permitted: (i) written consent of the database owner; (ii) the transfer of the information to a third party is performed lawfully, that is, based on the consent of the data subjects or is required by law; and (iii) If the information was transferred directly from Israel to such third party, such transfer itself would comply with the conditions set forth above.

On November 29, 2022, the Ministry of Justice published for public comments draft regulations on data transferred from the EEA to Israel which include additional data subject rights such as: right to be forgotten and restrictions on data retention, as part of Israel's deference to maintain its adequacy level of protection received from the EU. Timing of the regulations entering into force is dependent on the new government being formed.

On May 7, 2023, the Israeli Ministry of Justice published Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5783-2023, which establish obligations (such as: obligation to delete Personal Data, limit the retention of Personal Data that is not necessary, accuracy and notification obligations) that will apply to Personal Data transferred to Israel from the European Economic Area (EU, Iceland, Norway and Liechtenstein). Furthermore, information regarding a person's origin and information regarding membership in a labor organization will be considered Sensitive Data.

On September 14, 2023, the IPA published Manual: Contracting with Outsourcing Providers – Section 15 to the Data Security Regs, which clarifies the manner in which companies shall contract with their outsourcing providers. The manual specifies issues to be included in the binding agreement between the company and the outsourcing provider, and it includes two appendices for use by the parties: an auxiliary questionnaire for checking the information security aspects of the outsourcing provider, and a proposed questionnaire to determine the method of performing the periodic control of the outsourcing provider.

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. Similarly following the decision of the CJEH in the Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, IPA issued a statement on September 29, 2020, according to which US privacy shield 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.

On March 20, 2023, the IPA published Opinion: Security Risks in Shortened URLs, which describes the security risks arising from services that enable such shorten links to websites and recommends to avoid, unless a throughout security check has been conducted, not to apply such shortened links to a database of Personal Data and additional security related guidelines.

On September 7, 2023, the IPA published Guideline: The Role of The Board of Directors in Fulfilling The Corporation's Obligations According To The Privacy Protection Regulations (Information Security), which details the role of the board of directors in fulfilling the company's obligations according to the Data Security Regs. In companies which processing of Personal Data is at the core of their activity, or companies whose activity creates an increased risk of breaching privacy laws, the company's board of directors is the appropriate party to perform the duties set forth in the Data Security Regs.

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.

On August 7, 2022 the IPA updated their data breach notification policy. The IPA requires immediate reporting not only upon discovery, but also when there is merely a concern about the existence of a Serious Information Security Incident (as defined in the PPL), as well as the steps to be taken following the incident.

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 13th 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 opt-in 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.

In 2020, the Knesset approved Amendment 61 to the Consumer Protection Law, 5571-1981 ("Consumer Protection Law") which proposed to establish an opt-out arrangement for telephone marketing calls, known as "Do not call me" database, so that such calls could be held unless a consumer refused through active registration in the database. Consumers are able to register their phone numbers in the "Do Not Call Me" database from December 12, 2022.

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.