Data Protection and Privacy in Israel

Created on: ***11/20/2017***

by Amit Dat and Dr. Omri Rachum-Twaig, Fischer Behar Chen Well Orion & Co.

The Basic Laws of Israel that comprise the county's constitution specifically grant Israel's citizens the right to privacy as a basic human right. This practice note provides an overview of the regulation of data protection and privacy in Israel, presented in a question and answer format.

Legislative Framework

• **Question 1:** Summarize the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

Answer: The right to privacy is a constitutional right under Israeli law, and is specifically mentioned as one of the basic rights under the Basic Law: Human Dignity and Freedom. Principle 7 of the Basic Law: Human Dignity and Freedom states:

(a) Every person has a right to privacy and to intimacy in his life.

(b) There shall be no entry into the private premises of a person, without his permission.

(c) No search shall be held on the private premises of a person, upon his body, in his body, or among his private effects.

(d) The confidentiality of conversations of a person, his writings or his records shall not be violated.

The Protection of Privacy Law, 1981 and its associated regulations (collectively, the "Privacy Law") comprise the basic statutory framework for the protection of PII in Israel. The Privacy Protection Authority is an agency of the Israeli Ministry of Justice that enforces the right to privacy in accordance with the Privacy Law. Established in 2006, the Privacy Protection Authority issues guidelines that clarify and explain its interpretation of the Privacy Law.

Data Protection Authority

• **Question 2:** Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

Answer: The Privacy Protection Authority oversees compliance with the provisions of the Privacy Law and acts as Israel's Registrar of Databases. For this purpose, the Privacy Protection Authority is authorized to:

- Demand that any person or entity provide it with information and documents relating to a database
- Enter into a place where it has a reasonable basis for presuming that a database is being operated, to conduct a search, and to confiscate any object if it believes that it is necessary to do so in order to ensure the implementation of the Privacy Law and prevent its violation

Breaches of Data Protection

- **Question 3:** Can breaches of data protection lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Answer: The Privacy Protection Authority has the authority to enforce the Privacy Law as follows:

- **Database registration.** If the owner of a database breaches any provision of the Privacy Law, or does not comply with any demand made by the Privacy Protection Authority, the Privacy Protection Authority is entitled to postpone the validity of registration of the database for a period that the Privacy Protection Authority determines, or to cancel the registration of the database, provided that an opportunity was given to the owner of the database to present its claims.
- **Administrative fines.** In addition, the Privacy Protection Authority has the authority to impose administrative fines with respect to certain breaches of the Privacy Law.
- **Criminal liability.** The intentional violation of privacy, as well as the breach of some of the regulatory duties under the Privacy Law, are considered criminal offences, and committing them may be subject to criminal penalties.

Rights protected under criminal law are enforced by the Israeli Police, State Attorneys, and the Privacy Protection Authority (which functions as the legal branch of the State Attorney with respect to privacy matters), and later reviewed by the judicial system.

Rights protected under civil law are enforced by the data subjects themselves (e.g., as class actions under certain circumstances) and reviewed by the judicial system. Rights protected under administrative law are enforced by the Privacy Protection Authority.

Exempt Sectors and Institutions

- **Question 4:** Does the data protection law cover all sectors and types of organization or are some areas of activity outside its scope?

Answer: Yes. The Privacy Law covers all sectors, including governmental entities. The Privacy Law only exempts certain law enforcement and security agencies specified in the Privacy Law, and any person or entity acting on their behalf.

Communications, Marketing, and Surveillance Laws

- **Question 5:** Does the data protection law cover interception of communications, electronic marketing, or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Answer: The Privacy Law covers electronic marketing in the context of Direct Mailing (as defined below), and surveillance of individuals.

Other laws that regulate the interception of communications, monitoring, and other aspects of electronic marketing include:

- The Wiretapping Law, 1979
- The Communications Law (Telecommunications and Broadcasting), 1982
- The Consumer Protection Law, 1981
- The Computers Law, 1995

Other Laws

- **Question 6:** Identify any further laws or regulations that provide specific data protection rules for related areas.

Answer: There are sector-specific laws that provide additional protection for certain types of information. These include the following:

- Patients' Rights Law, 5756-1996 (medical information)
- Genetic Information Law, 5760-2000 (genetic information)
- The Psychologists' Law, 5737-1977 (information disclosed in the context of psychological treatment)
- The Banking Ordinance, 5701-1941 (financial data)
- The Credit Information Service Law, 5762-2002 and the Credit Data Law, 5776-2016 (credit information)

In addition, the following regulations were promulgated under the Privacy Law:

- Protection of Privacy Regulation (Information Security), 2017 (focusing on information security duties)
- Protection of Privacy Regulation (Transfer of Information to Databases Outside of Israel), 2001 (focusing on the legal basis for cross-border transfers of information)
- Protection of Privacy Regulation (Determining Databases Including Information that May Not Be Disclosed), 1987 (apply mainly to governmental entities)
- Protection of Privacy Regulation (Conditions to Holding Information and Transferring It between Governmental Bodies), 1986 (apply to governmental entities)
- Protection of Privacy Regulation (Conditions to Review of Information and Procedures for Appeals on Refusal to Review Requests), 1981

Furthermore, the Privacy Protection Authority publishes guidelines regarding its interpretation of the Privacy Law and its regulations, including the:

- Use of surveillance cameras and CCTVs
- Use of outsourcing services for the processing of PII
- Right of data subjects to remotely review their digital PII
- Use of PII for direct mailing services

PII Formats

- **Question 7:** What forms of PII are covered by the law?

Answer: The Privacy Law defines two types of PII with respect to provisions relating to digital databases:

- **Information.** Information means data about a person's personality, personal status, his private affairs, the state of his health, his financial situation, professional training, opinions, and beliefs.
- **Sensitive information.** Sensitive information means data about a person's personality, his private affairs, the state of his health, his financial situation, opinions, and beliefs. In other words, sensitive information includes all PII types covered by the term information except for "data about personal status and professional training." Note that recent court decisions have broadly interpreted these terms.

Extraterritoriality

- **Question 8:** Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Answer: The territorial scope of the Privacy Law is unclear. While the Privacy Law does not specifically determine any extraterritorial applicability, courts in recent years tend to decide, at least at the preliminary stage of the proceedings, that multinational organizations acting in Israel and collecting PII on Israeli citizens and residents are subject to the jurisdiction of Israeli courts and, in some circumstances, to the provisions of the Privacy Law.

This is based on the premise that when an Israeli resident's right to privacy is violated via the Internet, at least part of the infringing act occurs in Israel and is therefore subject to Israeli law. In a pending class action proceeding, the Supreme Court of Israel is expected to decide whether the jurisdiction and choice of law clauses of a multinational social network, that set forth a foreign jurisdiction for Israeli users, are valid and enforceable, and if not, which substantive law applies to these circumstances.

Covered Uses of PII

- **Question 9:** Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners?

Answer: Yes, all processing of PII is covered by the Privacy Law, except for the specific exemptions detailed in Question 4 above. Both owners (controllers) and holders (processors) of PII and databases are subject to the same duties under the Privacy Law. The main distinction is that the duty to register a database only applies to database owners.

Legitimate Processing (Grounds)

- **Question 10:** Does the law require that the holding of PII be legitimized on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Answer: The main basis for using PII under the Privacy Law is informed consent. In principle, PII cannot be collected or used without the data subject's informed consent. The Privacy Law defines "consent" as both implicit and explicit consent. The question of whether the obtained consent is sufficient is context specific.

The principle of consent is accompanied by the purpose limitation principle. In this sense, PII can only be used for the purpose for which the data subject agreed to its collection and use.

Legitimate Processing (Types of Data)

- **Question 11:** Does the law impose more stringent rules for specific types of PII?

Answer: While the Privacy Law itself does not impose specific rules with respect to specific types of PII, courts did review the consent of data subjects under more stringent rules regarding different classes of data subjects.

For example, in the context of labor relations, due to the structured asymmetry in the labor relation framework, the obligations of owners, holders, and managers of databases are subject to a higher standard of care. When collecting PII from an employee, special emphasis will be given on the prior notice obligation, as well as to the due process of obtaining the employee's free, informed, and specific consent to any collection, use, storage, and transfer of such PII.

Note that although no explicit legislation or regulation currently exists with respect to PII collected about employees, Israeli courts and the Privacy Protection Authority have determined that consent given by an employee does not necessarily constitute a valid and freely given consent unless the employer can prove otherwise. Moreover, Israeli case law establishes a general principle regarding the legitimacy of collection of information about employees, so that such information may be collected only to the extent necessary for the employer's activities and not beyond such purpose.

Notification

- **Question 12:** Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Answer: Yes. The Privacy Law requires database owners who collect PII directly from data subjects to notify such data subjects of the collection, request their consent, and provide the following information:

- Whether the person is under a legal duty to provide the information or whether the information is provided voluntarily
- The purpose for which the information is required
- The details of any third party that will receive the data, and for what purpose

Exemption from Notification

- **Question 13:** When is notice not required?

Answer: The notice requirement only applies to direct requests for the collection of PII made by the database owner. Therefore, when third parties provide PII about data subjects, such third parties are responsible to comply with this requirement. Note that the Privacy Protection Authority published draft guidelines regarding the duties that apply to prospective purchasers of databases, which include the duty to obtain the necessary assurances with respect to the legitimacy of the collection of PII included in such databases. In addition, specific regulations exist regarding the transfer of PII between governmental entities.

Control of Use

- **Question 14:** Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Answer: Please see answers to questions 10, 17, and 18.

Data Accuracy

- **Question 15:** Does the law impose standards in relation to the quality, currency, and accuracy of PII?

Answer: The Privacy Law entitles the data subject to request the amendment or deletion of any incorrect PII stored about that person. If the database owner refuses to amend the stored PII, it must inform the affected data subject within 30 days, and the data subject will then be entitled to commence a legal procedure in order to amend or delete the PII.

Amount and Duration of Data Holding

- **Question 16:** Does the law restrict the amount of PII that may be held or the length of time it may be held?

Answer: No. Note, however, that these parameters should be considered by the database owner as part of its duties under the Information Security Regulations, as described below.

Finality Principle

- **Question 17:** Are the purposes for which PII can be used by owners restricted? Has the "finality principle" been adopted?

Answer: As explained above, the consent requirement and the purpose limitation principles that apply under the Privacy Law, reflect the finality principle which was adopted, de facto, in Israel.

Use for New Purposes

- **Question 18:** If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Answer: The Privacy Law does not allow for PII to be used for purposes other than those for which it was collected and for which the data subject consented.

Security Obligations

- **Question 19:** What security obligations are imposed on PII owners and service providers that process PII on their behalf?

Answer: The Protection of Privacy Regulations (Information Security), 2017 (Information Security Regulations), promulgated under Section 17 of the Privacy Law, constitute a revolution in the regulation of information security in Israel and their application is far reaching.

The Information Security Regulations apply to any owner, holder, or manager of a database. Although the Information Security Regulations do not establish what specific technical information security measures a database owner must adopt, they do mandate the adoption of a series of corporate and managerial measures, as well as technological measures, that conform to the types of information that the organization stores and the uses that are made of the PII.

Therefore, the Information Security Regulations demand that each company must carry out its own internal assessment and preparation, including:

- Adopting a comprehensive policy and procedure on information security
- Mapping out the information systems in the organization and carrying out a risk assessment review
- Implementing information security practices in the area of human resources management

In addition, for databases containing PII that is of higher sensitivity, the Information Security Regulations require undertaking vulnerability assessments and penetration tests, and the implementation of advanced security mechanisms.

Notification of Data Breach

- **Question 20:** Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Answer: The Privacy Law does not include notification requirements regarding data breaches. However, the Information Security Regulations require database holders of certain sensitivity levels to notify the Privacy Protection Authority of data breaches. The Privacy Protection Authority has the authority to then require the database owners to further notify the data subjects themselves of such breaches.

In addition, sector-specific guidelines require certain entities to notify their applicable regulator with respect to information security incidents, such as data breaches. These include the banking, insurance, medical, and critical infrastructure industries. For example, the Israeli securities law requires that publicly traded companies disclose information about events that materially affect their business. Although data breach notifications are not specifically required under such law, such incidents must be disclosed if they are material to the company's business.

Data Protection Officer

- **Question 21:** Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

Answer: No. While the database registration process does require the database owner to appoint a database manager, and while such database manager is personally liable for some of the requirements under the Privacy Law, there is no duty to appoint a data protection officer. Note that the owners of five databases or more are required to appoint an Information Security Manager with respect to databases containing PII. The Information Security Regulations determine that once an Information Security Manager is appointed, it must be independent of other conflicting duties and to report directly to a member of the company's executive management.

Recordkeeping

- **Question 22:** Are owners of PII required to maintain any internal records or establish internal processes or documentation?

Answer: The Privacy Law does not require database owners to maintain internal records regarding the collection and storage of PII. However, the Information Security Regulations require database owners to maintain some internal records, processes, and documentation regarding their databases.

Registration

- **Question 23:** Are PII owners and/or processors of PII required to register with the supervisory authority? Are there any exemptions?

Answer: Yes. You must register a database at the Registry of Databases administered by the Privacy Protection Authority in certain cases set forth in the Privacy Law, including when a database contains one of the following:

- PII about more than 10,000 people
- Sensitive information (as defined above)

- PII that was not provided by the data subject, on the subject's behalf, or with the subject's consent
- The database is used for Direct Mailing Services (as defined below)

The obligation to register a database does not apply to any of the following:

- A database that contains PII that was made public in accordance with an official legal authorization
- Databases only used for personal purposes
- Databases that only include names, addresses, and means of communication, which in and of themselves do not generate a feature that could adversely affect the privacy of the people whose names are included therein, and provided that neither the owner of the database nor an entity under the owner's control has an additional database in its possession

In addition, the Privacy Law authorizes the Privacy Protection Authority, for special reasons that must be recorded, to require the registration of a database that otherwise would be exempt from registration.

Formalities

- **Question 24:** What are the formalities for registration?

Answer: You must submit the following details to the Privacy Protection Authority:

- The identity of the owner, holder, and the manager of the database
- The purpose of collecting and using the PII to be stored in the database
- The type of PII that will be included in the database
- Details regarding the source of PII
- Details regarding the transfer of PII to third parties, including outside Israel (to the extent relevant)
- The number of data subjects and users of the databases, and technical details with respect to the infrastructure of the database
- A copy of the privacy policy or the letter of consent executed by the data subject

In certain cases, additional information may be required. For example, if the database is used for Direct Mailing, a copy of the specific form of Direct Mailing is required.

The Privacy Protection Authority will register the database in the registry within 90 days from the date of its submission, unless the Privacy Protection Authority has a reasonable basis to believe that the database has been used or could be used for illegal or camouflaged activities, or that the PII included in the database was not assembled or collected in accordance with the Privacy Law. If the Privacy Protection Authority does not register the database within 90 days and does not inform the applicant of the refusal to register the database or of the delay in the registration, the applicant is entitled to administer or to use the database, even if it has not been registered.

The Privacy Protection Authority is authorized to register a different purpose from the purposes indicated by the applicant or to order the submission of multiple registration requests, if the Privacy Protection Authority believes such steps to be appropriate in view of the actual uses of the database. The Privacy Protection Authority may not refuse to register the database unless a right to a hearing and an opportunity to provide comments are provided to the applicant.

The registration and maintenance fees for databases were recently repealed, and as of today, no fees are required for the registration of databases in Israel.

Penalties

- **Question 25:** What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Answer: The criminal liability for failing to register a database in accordance with the Privacy Law is one year imprisonment. In addition, the Privacy Protection Authority may issue an administrative fine in the amount of up to NIS 25,000 per violation with respect to companies and NIS 5,000 with respect to individuals.

Refusal of Registration

- **Question 26:** On what grounds may the supervisory authority refuse to allow an entry on the register?

Answer: The Privacy Protection Authority may refuse to allow an entry to the register if it has reasonable grounds to believe that the database is used or may be used for illegal activities, or that the PII included in it was received, aggregated, or collected in violation of the Privacy Law or any other applicable law.

Public Access

- **Question 27:** Is the register publicly available? How can it be accessed?

Answer: Yes. The register can be publicly searched on the Privacy Protection Authority's website. Such open search provides extracts of the registration certificates. Full information on registered databases can be obtained by contacting the Privacy Protection Authority via mail or e-mail.

Effect of Registration

- **Question 28:** Does an entry on the register have any specific legal effect?

Answer: The main legal effect of an entry on the register is compliance with the registration requirement under the Privacy Law. The substantive duties of database owners apply regardless of the registration status of the database.

Transfer of PII

- **Question 29:** How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Answer: Guidelines 2/2011 on the Use of Outsourcing Services, issued by the Privacy Protection Authority (Outsourcing Guidelines), require certain organizational and contractual measures to be taken, including the following:

- **Examination.** The owner/holder (Commissioning Party) must examine, prior to the engagement with a third-party provider, whether the outsourcing is appropriate considering the:
    - Nature of the PII in the database
    - Service provider's previous experience, background, and reputation –and–
    - Risk of a conflict of interest with the service provider
- **Engagement agreement.** The engagement agreement between the parties must include provisions regarding the service provider's obligations for the safeguarding and use of the database and PII, as required under the Privacy Law, including the:

- Nature and scope of the services, the permitted use of the PII, and the identity of the employees and/or sub-contractors who will have access to the PII
- Service provider's obligation to secure the PII and its confidentiality –and–
- Commissioning Party's ability and right to monitor and inspect the service provider, and effective remedy

In addition, the agreement must include:

- A binding security appendix
- Obligations of the service provider not to transfer PII to third parties or use the PII for any purpose other than the purpose defined in the agreement –and–
- Procedures regarding the rights of the subjects of the PII, including with respect to review, amendment and deletion of the PII

- **Limited duration.** The agreement must provide that the service provider will keep the PII only for the time needed to complete its obligations under the agreement. Upon termination of the agreement, the Commissioning Party will verify that the service provider has deleted all the PII, and if the service provider needs the PII in order to defend itself against any claims, a copy of the PII may be maintained with a trustee.

Restrictions on Disclosure

- **Question 30:** Describe any specific restrictions on the disclosure of PII to other recipients.

Answer: The Privacy Law sets forth that the owner and holder of a database and all of their employees are obligated to maintain the confidentiality of the PII included in the database. This means that the disclosure of PII is subject to the consent of the data subject, except for disclosure that is required for the purpose of complying with any specific requirement under the Privacy Law or according to a court order.

Cross-Border Transfer

- **Question 31:** Is the transfer of PII outside the jurisdiction restricted?

Answer: Yes. The Privacy Protection Regulations (Transfer of Personal Information to Databases Outside the State Borders) – 2001 (the Transfer Regulations) provide that no person can transfer PII from databases located in Israel to other jurisdictions, unless the law in the jurisdiction to which the PII is transferred provides the same level of privacy protection as Israel.

The Transfer Regulations set forth specific additional circumstances in which the transfer of PII outside of Israel is allowed. These include the following:

- The data subject agreed to the transfer of his/her PII
- It is not possible to obtain the consent of the data subject and the transfer is necessary to protect the subject's health
- The PII is transferred to a corporation controlled by the owner of the database (who transfers the PII) and such corporation agreed to protect the privacy of the PII following the transfer
- The PII is transferred to a third party who agrees to provide the same level of data protection required under Israeli law, *mutatis mutandis*
- The PII was released to the public, under lawful authority
- The transfer of PII is necessary to protect public safety
- The transfer of PII is required under Israeli law
- The PII is transferred to a country that:

- Is a party to the European Directive for Protection of Individuals with Regard to Automatic Processing of Sensitive Information
- Is receiving PII from states that are members of the European Union
- Has been confirmed, by publication of the Privacy Protection Authority, to have a governmental body that protects privacy, and a cooperation agreement between the Privacy Protection Authority and such governmental body has been executed

Following the judgment of the Court of Justice of the European Union (CJEU), in which the Safe Harbor Agreement between the United States and EU was declared invalid, the Privacy Protection Authority issued a clarification that a transfer of PII to the United States based solely on subsection (h)(ii) does not meet the requirements of the Transfer Regulations. The Privacy Protection Authority further clarified that the Transfer Regulations contain additional alternative paths for transferring PII outside of Israel, including to the U.S. Note that although no formal clarification was yet published by the Privacy Protection Authority, the new Privacy Shield framework may meet the requirements of the Transfer Regulations, under subsection h(ii), regarding PII transfer from Israel to the United States.

Notification of Cross-Border Transfer

- **Question 32:** Does cross-border transfer of PII require notification to or authorization from a supervisory authority?

Answer: No.

Further Transfer

- **Question 33:** If transfers outside the jurisdiction are subject to restriction or authorization, do these apply equally to transfers to service providers and onwards transfers?

Answer: The Transfer Regulations prohibit the onward transfer of PII. Therefore, service providers to whom PII was transferred from Israel are prohibited from making onward transfers of such PII.

Access

- **Question 34:** Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Answer: Yes. Database owners and holders must allow the data subjects to review their PII kept in the database, except in the following cases:

- The PII relates to medical or psychological state of the data subject, and such PII may cause damage to the physical or mental health of the data subject or risk to the subject's life (in such a case, the PII will be provided to the physician or psychologist of the subject of information)
- The PII is privileged under applicable law
- The database is owned by certain governmental bodies and law enforcement agencies listed in the Privacy Law

In accordance with Guidelines number 1/2017, issued by the Privacy Protection Authority, the review and access obligations of a database owner or holder also apply to recorded calls, chat correspondences, videos, and other PII stored by digital means. In addition, under these Guidelines the owner and holder shall enable the review by the data subject via remote means, as applicable.

Other Rights

- **Question 35:** Do individuals have other substantive rights?

Answer: No.

Compensation

- **Question 36:** Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Answer: Yes. Various violations of the Privacy Law constitute civil torts and may entitle the plaintiff to damages. The plaintiff can choose between actual damages that must be proved by evidence and statutory damages, which the court may determine in an amount of up to NIS 50,000 for non-intentional violations of privacy and up to NIS 100,000 for intentional violations of privacy.

Enforcement

- **Question 37:** Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Answer: Both. As described above, the various rights under the Privacy Law and its underlying regulations are protected under criminal law, civil law, and administrative law. Rights protected under criminal law are enforced by the Israeli Police, State Attorneys, and the Privacy Protection Authority (which functions as the legal branch of the State Attorney with respect to privacy matters), and later reviewed by the judicial system. Rights protected under civil law are enforced by the data subjects themselves (e.g., as class actions under certain circumstances) and reviewed by the judicial system. Rights protected under administrative law are enforced by the Privacy Protection Authority.

Further Exemptions and Restrictions

- **Question 38:** Does the law include any derogations, exclusions, or limitations other than those already described? Describe the relevant provisions.

Answer: The Privacy Law provides the following defenses from liability:

- The violation of privacy was done through a protected publication under the Israeli Libel Law, 1965
- The infringing party performed the violation in good faith under one of the following circumstances:
    - He did not know and was not supposed to know about the potential violation
    - It was committed in circumstances under which the infringer has a legal, moral, social, or professional duty to do so
    - It was committed in order to protect a legitimate interest of the infringer
    - It was committed in the lawful ordinary course of business of the infringer and was not publicly disclosed –or–
    - It was committed through the photography or publication of photographs taken in public places in which the plaintiff appeared incidentally
- There was a public interest justifying the violation, and if it was performed by publication, the publication was truthful

Judicial Review

- **Question 39:** Can PII owners appeal against orders of the supervisory authority to the courts?

Answer: Yes. As with any administrative authority in Israel, decisions of the Privacy Protection Authority could be appealed against through a petition to the competent Administrative Courts in the relevant jurisdiction. Such petition must be filed no later than 45 days from the date on which the decision of the Privacy Protection Authority was published or delivered to the petitioner. The petitioner has the right to appeal against the Administrative Court's decision to the Supreme Court of Israel.

Internet Use

- **Question 40:** Describe any rules on the use of "cookies" or equivalent technology.

Answer: Currently, no specific regulation of the use of cookies exists in Israel, and the Privacy Law and the regulations promulgated thereunder apply to the use of cookies in the same manner they apply to any other type of PII.

Electronic Communications Marketing

- **Question 41:** Describe any rules on marketing by e-mail, fax, or telephone.

Answer: The Privacy Law imposes certain obligations with respect to databases that are used for Direct Mailing and Direct Mailing Services (as defined below). For example, any approach to a person in a Direct Mailing requires a notice that will disclose the fact that it is a Direct Mail, the sources of the PII used for the Direct Mailing, the rights of the data subject to be deleted from the database or applicable mailing list, and similar matters.

Direct Mailing should be distinguished from spam activities. The term Direct Mailing is defined as "any personal approach to a person, based on his belonging to a certain group in the population, determined according to a categorization of the data subjects included in the database." The term "Direct Mailing Services" is defined as "Direct Mailing services to others by providing lists, stickers or other PII to others for the purpose of Direct Mailing."

In addition to the Privacy Law, Section 30A of the Israeli Communications Law (Telecommunications and Broadcasting), 1982 (Anti-Spam Law) provides a general prohibition on the publication of Advertisement be means of distribution of spam messages.

An "Advertisement" is defined as a "commercially distributed message which purpose is to encourage the acquisition of a product or service or the expenditure of moneys in any other way. . .." An "Advertiser" is defined as "the person whose name or address appear in the Advertisement for communication purposes or for the acquisition of the subject of the Advertisement, whoever the content of the Advertisement may publish its business . . . or whoever markets the subject of the Advertisement of another person. . .."

The general prohibition is on the communication of Advertisements by an Advertiser, using certain technological means, without the explicit consent of the recipient. In addition, even if consent of the recipient is obtained, the Anti-Spam Law requires that any Advertisement sent to a recipient will include the word Advertisement" in the subject line as well as the contact details of the Advertiser and the option for the recipient to unsubscribe from receiving future Advertisements.

Cloud Services

- **Question 42:** Describe any rules or regulator guidance on the use of cloud computing services.

Answer: The Privacy Law and its underlying regulations do not specifically address cloud computing services. The Privacy Protection Authority published several guidelines that indirectly apply to cloud computing services. For example, the Privacy Protection Authority specifically explained that the Outsourcing Guidelines apply to cloud computing services. In addition, the Privacy Protection Authority published specific instructions with respect to the registration process of databases that are stored using cloud storage services.

Updates and Trends

- **Question 43:** Identify recent updates and trends.

Answer: Three recent changes are noteworthy.

First, the Information Security Regulations, as described above, were recently promulgated and will enter into force in May 2018. This is a landmark change in the field of data protection and information security in Israel and will significantly impact the Israeli market with respect to the protection of PII.

Second, the Privacy Protection Authority and Israeli Ministry of Justice recently repealed the Protection of Privacy Regulations (Fees), and effectively abolished the database registration and maintenance fees. This is part of the Privacy Protection Authority's agenda to reduce the formalities associated with the registration of databases, and focus on the enforcement of the substantive duties of database owners and holders.

Third, the Privacy Protection Authority recently published draft guidelines on the ownership transfer and change of databases. The draft guidelines require database owners and prospect transferees to meet certain requirements, including, in some circumstances, obtaining the updated consent of the data subjects for the new ownership of the database. If these draft guidelines come into effect, they are expected to impact a significant portion of M&A transactions involving the change of ownership of databases.