Data Protection: Israel

HAIM RAVIA AND DOTAN HAMMER, PEARL COHEN ZEDEK LATZER BARATZ, WITH PRACTICAL LAW

A Q&A guide to data protection in Israel. This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects; rights to access personal data or object to its collection; and security requirements. It also covers cookies and spam; data processing by third parties; and the international transfer of data. This article also details the national regulator; its enforcement powers; and sanctions and remedies. To compare answers across multiple jurisdictions, visit the Data protection Country Q&A tool.

REGULATION

LEGISLATION

1. What national laws regulate the collection and use of personal data?

General laws

In Israel, Article 7 of Basic Law: Human Dignity and Liberty (5752-1992) (unofficial translation) establishes a constitutional right to privacy. In addition, Israeli law includes an omnibus privacy and data protection statute, the Protection of Privacy Law (5741-1981) (*PPL*) (unofficial translation). The PPL includes:

- A privacy regime addressing invasion of privacy.
- A personal data protection regime addressing the use of databases containing personal data.

The PPL does not incorporate EU Data Protection Directive (95/46/EC), other than implicitly referencing it in the PPL's regulations governing cross-border transfer of data (*see Question 20*).

Various regulations promulgated under the PPL set out rules and procedures for, amongst others:

- Data security.
- Retaining and safeguarding personal data.
- Granting data subjects right to access, amend, and delete personal information.
- Cross-border transfer of personal data.

The Registrar of Databases (*Registrar*) occasionally releases guidelines on data protection and privacy. These guidelines are not legally binding, but do:

- Represent the Registrar's interpretation of the PPL.
- Serve as guiding principles for the Registrar's exercise of enforcement powers.

For more information on the Registrar, see *Question 25*.

Sectoral laws

Israeli law also includes a number of sectoral legislations on privacy and data protection matters. The main sectoral laws are:

- The Patient Rights Law 5756-1996, which governs medical treatment of patients and protection of patients' medical and health information.
- The Genetic Information Law 5761-2000, which governs the collection, use, and handling of genetic information.
- The Credit Data Services Law 5762-2002, which governs the collection and dissemination of data regarding the creditworthiness of individuals and sole proprietors. This law will be substituted by the Credit Data Law 5776-2016, within about two years.
- The Biometric Database Law, which establishes a national database containing the biometric data of all Israeli citizens.
- The Criminal Procedure Law (*Enforcement Powers-Communication Data*) 5768-2007, which governs the access to telecom meta-data by the police and various other investigative and security agencies.

© 2017 Thomson Reuters. All rights reserved.

SCOPE OF LEGISLATION

2. To whom do the laws apply?

The Protection of Privacy Law 5741-1981 (*PPL*) confers the right to privacy and data protection on individuals, referred to as data subjects. The PPL's protections do not extend to legal persons, such as corporations.

The duties and obligations under the PPL apply to:

- Database owners, who have the primary title and interest in a database (*see Question 3*).
- Database holders, who are persons or entities with regular possession of the database (or a copy of it) and are permitted to use the database.
- Database managers, who are either:
  - active officers in an organization that owns or holds a database; or
  - such other person that the officer has authorized to act in this manner.

Database owners and holders may be:

- Individuals.
- Legal persons.
- The state.

For more on the definition of personal data, see *Question 3*. For more on data processing operations, see *Question 4*.

3. What data is regulated?

The data protection regime of the Protection of Privacy Law 5741-1981 (*PPL*) regulates personal data processing. It protects databases, which are collections of information elements held in a magnetic or optical medium and intended for computerized processing (personal information), with some limited exceptions.

Under the PPL, personal information includes data pertaining to an individual's:

- Personality.
- Familial status.
- Intimate affairs.
- Health or medical condition.
- Financial status.
- Professional qualifications.
- Opinions or beliefs.

Sensitive information is a subset of personal information that covers data about an individual's:

- Personality.
- Intimate affairs.
- Health or medical condition.
- Financial status.
- Opinions and beliefs.

The distinction between personal information and sensitive personal information impacts:

- The triggering criteria for compulsory registration databases with the Registrar of Databases (*see Question 6*).
- The level of data security required under the data security regulations (*see Question 19*).

Israeli case law interpreting the PPL extends regulated data beyond the foregoing definitions by protecting the private affairs of an individual. According to the Israeli Supreme Court, private affairs comprise all information relating to an individual's private life, including:

- The individual's:
  - name;
  - address; and
  - contact information.
- The details of the individual's workplace, friends, and family.

Various sectoral laws protect other specific information of individuals (*see Question 1*).

4. What acts are regulated?

The database regime of the Protection of Privacy Law 5741-1981 (*PPL*) regulates the collection of information for the purpose of maintaining it in a database. The PPL also regulates:

- Processing activities subsequent to the initial collection.
- Cross-border transfer of personal information from a database (*see Question 19*).
- Information security measures to be taken with respect to personal information (*see Question 19*).
- Rights granted to data subjects (*see Question 15*).
- Use of databases for direct mailing purposes, defined as contacting a person (such as by written communications, telephone, fax, or computerized means) under some characteristic-based profiling or segmentation.

The PPL specifically prevents the following activities if conducted without consent:

- Spying on or trailing a person in a manner likely to harass him.
- Wiretapping.
- Photographing an individual when the individual is in a private domain, or publishing a photograph of an individual taken in public, if the publication may shame or scorn the individual.
- Copying the contents of a letter or other message not intended for publication, or using those materials without the permission of the addressee or the author.
- Breaching confidentiality obligations set out under law or agreement.
- Using, disclosing, or transferring information regarding the private affairs of an individual, for purposes other than for which the information was given.

© 2017 Thomson Reuters. All rights reserved.

5. What is the jurisdictional scope of the rules?

Israeli law does not clarify the jurisdictional scope of the rules. For example, it is unclear whether the requirements concerning a database also apply to a database containing personal data of Israelis that is owned, held, and processed outside Israel by an entity incorporated outside Israel.

6. What are the main exemptions (if any)?

The following two categories of databases are exempted from the database regime of the Protection of Privacy Law 5741-1981:

- A database maintained for personal use and not for business purposes.
- A database that by itself does not create any characterization that may invade the privacy of data subjects, if the:
  - database includes only names, addresses, and contact information; and
  - database owner and any subsidiary or other entity it controls has no other database.

There are also certain exemptions from the statutory requirement to register a database with the Registrar of Databases. For more information on registration, see *Question 7*.

NOTIFICATION

7. Is notification or registration required before processing data?

Before using a database, database owners must register their databases with the Registrar of Databases (*Registrar*) if any of the following is true:

- The number of data subjects in the database exceeds 10,000.
- The database includes personal information that was not provided by the data subjects, on their behalf or with their consent.
- The database includes sensitive information (*see Question 3*).
- The database is used to provide direct mailing services to others.

To register, database owners must file a registration application and pay a filing fee. Application forms are in Hebrew and can be submitted online through the Registrar's website (*see box, Regulator details*). The registration application requires numerous details regarding the database, including:

- The purposes of the database.
- The data collection methods.
- The text of the notice given to data subjects and the applicant's process for obtaining the data subjects' consent.
- Details regarding cross-border data transfer.

If the Registrar does not register a database within 90 days of submission of an application, the database owner generally may begin using the database without approval.

Owners of registered databases must also update their registration if there are changes to details regarding the database. Annual recurring fees also apply.

MAIN DATA PROTECTION RULES AND PRINCIPLES

MAIN OBLIGATIONS AND PROCESSING REQUIREMENTS

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

Under the Protection of Privacy Law 5741-1981 (*PPL*), the main obligations imposed on database owners are to:

- Provide notice to data subjects before collecting and processing their data (*see Question 12*).
- Facilitate the data subjects' right to review, correct, and delete their personal data (*see Question 13*).
- Safeguard the database (*see Question 15*).
- Comply with the requirements for cross-border transfer of personal data (*see Question 20*).
- Register their databases in certain circumstances (*see Question 7*).

Under the PPL, database holders must ensure that access to each database is granted only to those explicitly authorized in a written agreement between the holder and the owner of each database. The PPL also requires any holder of five or more databases to annually report to the Registrar of Databases:

- A list of databases in its possession, indicating the owners of the databases.
- An affidavit attesting that those authorized to access each database have been designated in agreements between the holder and the owner.
- The name of the person in charge of the database's security.

Additional obligations apply to using personal data for direct mailing purposes.

9. Is the consent of data subjects required before processing personal data?

The Protection of Privacy Law 5741-1981 (*PPL*) requires both notice and consent. Any request made to data subjects that seeks personal information to use in a database must be accompanied by a notice containing certain disclosures detailed in *Question 12*.

Under the PPL, informed consent may either be explicitly obtained or inferred under the circumstances. If the required notice is properly drafted and communicated to data subjects, consent to data provided subsequent to notice may be inferred. The PPL does not preclude online notice and consent.

The PPL is silent on the collection and processing of personal data of minors. The general rules under the Israeli Legal Capacity and Guardianship Law 5722-1962 require parental consent to any activity or action with legal significance of an individual under the age of 18.

© 2017 Thomson Reuters. All rights reserved.

For more on required personal data processing disclosures, see *Question 12*.

10. If consent is not given, on what other grounds (if any) can processing be justified?

The Israeli privacy and data protection regime is based almost exclusively on the notions of notice and inferred or explicit informed consent of data subjects. For more information on consent, see *Question 9*.

Under appropriate circumstances, however, the Protection of Privacy Law 5741-1981 offers after-the-fact defenses to claims of invasion of privacy under which courts may find justifiable data processed without consent. These defenses may release a defendant from civil or criminal liability, or otherwise limit liability. For more information on sanctions and penalties, see *Question 26*.

SPECIAL RULES

11. Do special rules apply for certain types of personal data, such as sensitive data?

Under the Protection of Privacy Law 5741-1981, the collection and processing of sensitive information (*see Question 3*) triggers the statutory requirement to register databases with the Registrar of Databases. For more information on registration, see *Question 7*. Databases that include special categories of data are also subject to elevated data security obligations (*see Question 15*).

In addition, under the the Credit Data Services Law 5762-2002, entities that possess information on the creditworthiness of individuals and sole proprietors must make that information available to licensed credit reporting agencies, which are in turn authorized to disseminate the information subject to certain conditions and limitations. The law provides that these entities must get the subject's opt-in consent to collect certain forms of data.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

Any request made to data subjects seeking their personal information for use in a database must be accompanied by a notice containing the following elements:

- Information on whether the data subjects are under legal duty to provide the requested information or whether it is a product of choice and consent.
- The purposes for which the information is requested.
- To whom the information may be later transferred and the purposes of the transfer.

13. What other specific rights are granted to data subjects?

The Protection of Privacy Law 5741-1981 (*PPL*) grants data subjects the following rights:

- **Review and access**. Data subjects are entitled to review information about them maintained in a database, subject to certain limited exceptions.
- **Correction**. Data subjects may request the correction or deletion of incorrect, incomplete, unclear, or outdated information.

The PPL suggests that a database owner may decline requests to correct or delete personal data. However, the law does not specify the legally justifiable grounds for refusal.

The Registrar of Databases has issued guidelines on data subjects' right to review their personal data, including their:

- Customer service calls.
- Recordings, chats, and conversations.
- Video calls.
- Other digital information maintained by businesses providing services to the public.

According to the guidelines, the right of access applies when the data that the organization maintains can be correlated to the inquiring individual using reasonable measures or efforts, even if the data was not initially indexed in an identifiable manner. Access should be given after appropriate measures are taken to identify the data subject.

14. Do data subjects have a right to request the deletion of their data?

Data subjects have a right to request the deletion of their data under restricted circumstances when the data is found to be erroneous (*see Question 13*).

SECURITY REQUIREMENTS

15. What security requirements are imposed in relation to personal data?

The Protection of Privacy Law 5741-1981 (*PPL*) imposes a specific set of security requirements on database managers. A database manager is an active officer in an organization that owns or holds a database or such other person that the officer has authorized to act as such. The database manager has primary responsibility for the information security of a database, though database owners and holders must still ensure compliance with security requirements under the PPL.

In addition, the PPL requires that any person or entity that holds five or more databases appoint an information security officer. The PPL does not elaborate on the required qualifications of an information security officer, other than requiring them to be a suitably trained person.

The data security regulations specify a partial, but non-exhaustive, list of procedures that the database manager should employ to secure information. Some of the key procedures include:

- Employing reasonable security measures, commensurate with the sensitivity of the information, to prevent inadvertent or deliberate intrusions to the database beyond the scope of a user's access privileges.

© 2017 Thomson Reuters. All rights reserved.

- Establishing procedures for detecting information integrity breaches and the remediation of such breaches.
- Establishing procedures for the management of the database, third party service providers, and instructions for collecting, marking, verifying, processing, and distributing the information, in accordance with the PPL and the regulations.
- Maintaining an updated list of users authorized to access the database, according to the various access privileges.
- Having authorized users execute confidentiality and non-use obligations.

Sectoral requirements exist as well. For example, the Supervisor of Banks issued a circular in 2015 on cyber-defense management at banking corporations and credit card companies (*2015 Circular*). The 2015 circular:

- Provides that banking corporations are expected to regularly identify and evaluate cyber threats and risks.
- Spells out the requirements for an effective process for identifying and evaluating cyber risks.
- States that banking corporations ought to continuously examine the effectiveness of their various cyber-defense controls using tools such as vulnerability reviews and controlled-intrusion tests.

In addition, in 2016, the Department of Capital Market, Insurance and Savings at the Israeli Ministry of Finance issued a circular (*2016 circular*) on cyber risk management at institutional entities regulated by the department. The 2016 circular will enter into force in 2017 and, amongst other instructions:

- Specifies that information risk management is an essential element in managing information technology.
- Aims to ensure the protection of rights afforded to consumers and policyholders by requiring institutional entities to safeguard the following:
  - data confidentiality;
  - integrity and availability of information assets;
  - data systems; and
  - business processes.
- Requires the institutions' board of directors and management to oversee ongoing information security activities and cyber risks and to guide and monitor the implementation of data security measures.

In March 2018, new data security regulations, the Protection of Privacy Regulations (Data Security), 5777-2017, will enter into effect. The Regulations classify databases into the following four categories, each subject to an escalating degree of information security requirement:

- Databases maintained by individuals or sole proprietors, subject to some exceptions. The security requirements for these databases are the most lenient.
- Databases subject to the basic level of data security requirements, which includes databases that do not fall within any of the other categories.
- Databases subject to the intermediate level of data security requirements, which includes databases:
  - to which more than 10 people have access credentials and whose purposes include making information available to other parties; and
  - maintained by public agencies, or databases that contain special categories of data, such as, among others, medical or health information, genetic or biometric data, and information about an individual's political opinions or financial status.
- Databases subject to the high level of data security requirements, including databases:
  - whose purposes include making information available to other parties, and in which either the number of data subjects is 100,000 or more or to which more than 100 people have access credentials; and
  - with special categories of data and in which either the number of data subjects is 100,000 or more or to which more than 100 people have access credentials.

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

The forthcoming information security regulations taking effect in March 2018 (*see Question 15*) will require database owners and holders to notify the Registrar of Databases (*Registrar*) of security breaches in the following cases:

- Databases subject to the intermediate level of data security (*see Question 15*) will be required to notify the Registrar in any of the following instances:
  - any severe data breach in which a material part of the database was access or used without authorization, or in the course exceeding authorized access; and
  - any severe data breach in which the database's integrity was compromised.
- Database owners subject to the high level of data security will be required to notify the Registrar of any severe data breach in which any portion of the database was breached, not just a material part.

In either case, the Registrar can then require that the database owner or holder notify data subjects.

In addition, both of the following sectoral directives require notification to the relevant regulator of breaches:

- 2015 Circular on cyber-defence management at banking corporations and credit card companies, for entities governed by the Supervisor of Banks (*see Question 15*).
- 2016 Circular on information risk management, for entities governed by the Department of Capital Market, Insurance and Savings at the Israeli Ministry of Finance (*see Question 15*).

PROCESSING BY THIRD PARTIES

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

In 2012, the Registrar of Databases (*Registrar*) published guidelines imposing a stringent set of requirements on organizations seeking to commission outsourcing services to process personal information (*Outsourcing Guidelines*).

© 2017 Thomson Reuters. All rights reserved.

The Outsourcing Guidelines require commissioning organizations to:

- Perform certain pre-engagement due diligence reviews.
- Enter into a written agreement with the data processing services provider.
- Impose numerous contractual obligations on the data-processing services provider.

Additional issues outlined in the Outsourcing Guidelines include:

- Establishing of information security measures.
- Servicing of providers' insurance coverage.
- Certain bans on transferring to others, or co-mingling, data obtained by virtue of an engagement with the commissioning organization.
- Rights of the Registrar and the commissioning organization to audit the service provider.

Certain aspects of these guidelines were recently codified into the binding Protection of Privacy Regulations (Data Security), which will enter into force in late March 2018 (see *Question 15*).

ELECTRONIC COMMUNICATIONS

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject's terminal equipment?

There are no specific legislative or regulatory rules for cookies. The general provisions of the Protection of Privacy Law 5741-1981 (*PPL*) apply to the use of cookies, to the extent the cookies collect or process personal information as defined in the PPL or information regarding an individual's private affairs. For more information on personal information and private affairs, see *Question 3*.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

The Israeli anti-spam law was introduced in 2008 as an amendment to the Communications Law (Telecom and Broadcasts) 5742-1982 (*Anti-Spam Law*). It takes an opt-in approach and prohibits the transmission of advertisements through any of the following, unless recipients have given their prior written consent:

- Fax.
- Email.
- Text messages (SMS).
- Robocalls.

An advertisement is defined as any of the following:

- A commercially distributed message whose purpose is to encourage the purchase of goods or services, or otherwise encourage expending money.
- A message distributed to the public for the purpose of donations or non-commercial marketing.

The definition of advertisements excludes political messages and election campaigns.

The Anti-Spam Law provides two limited exceptions to the fundamental opt-in rule, including the following:

- Non-profit advertisers may send emails promoting donations or non-commercial messages without the recipient's prior consent, if the recipient has not opted-out of these messages.
- Advertisers may send a one-time opt-in offer to businesses to seek their consent to receive advertisements, though under case law the offer itself may not be an advertisement.

Advertisers must also indicate an unsubscribe option in each advertisement.

INTERNATIONAL TRANSFER OF DATA

TRANSFER OF DATA OUTSIDE THE JURISDICTION

20. What rules regulate the transfer of data outside your jurisdiction?

The Protection of Privacy Law 5741-1981 (*PPL*) restricts cross-border transfer of personal data originating from databases in Israel unless the law of the destination jurisdiction both:

- Provides a level of data protection no lesser than the level of protection prescribed by Israeli law.
- Abides by the following data protection principles:
  - fair processing;
  - purpose limitation;
  - data accuracy;
  - data subjects' rights to review and correct data; and
  - information security safeguards.

Nevertheless, the PPL provides certain exceptions that permit cross-border transfer of personal data to jurisdictions whose laws do not mandate the foregoing required principles. For instance, cross-border transfer of data may be permissible if:

- The data subject consents to the transfer.
- The data is transferred to a foreign affiliate controlled by the corporation from which the data transfer originates.
- The data is transferred to a person contractually bound to comply with the same conditions for possession and use of personal data that apply to a database in Israel, with necessary changes taken into account.
- The data is transferred to a jurisdiction that:
  - is a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data; or
  - receives personal data from EU member states under the EU's applicable terms for cross-border transfer of personal data.

Israeli regulations set out additional, conjunctive requirements to cross-border data transfers. They require the database owner from which the data transfer originates to bind the foreign data recipient to a written data transfer agreement. Under the data transfer agreement, the recipient must agree:

© 2017 Thomson Reuters. All rights reserved.

- To employ sufficient means to ensure the privacy of data subjects.
- That the personal data will not be transferred onwards to any other person or entity, whether in that same country or another country.

21. Is there a requirement to store any type of personal data inside the jurisdiction?

There is no requirement to store personal data inside Israel, but restrictions on transferring personal data outside Israel apply (*see Question 20*).

In 2015, the Supervisor of Banks at the Bank of Israel issued guidelines regarding the use of cloud computing services. The guidelines provide that Israeli banks and credit card companies may use cloud services only if the data is stored both:

- In Israel.
- Through a cloud service provider that adequately protects personal data pursuant to EU Data Protection Directive (95/46/EC).

DATA TRANSFER AGREEMENTS

22. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

Israeli regulations require that a foreign recipient of personal data undertake specific written obligations (*see Question 20*). These can be formulated as a data transfer agreement, but there are no standard forms or precedents approved by the Israeli Law, Information, and Technology Authority (*ILITA*).

23. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

A data transfer agreement suffices if it both:

- Requires the data recipient to comply with the same conditions for possession and use of personal data that apply to a database in Israel.
- Includes other required written obligations.

For more information on the use of data transfer agreements to legitimise transfer, *see Question 20*.

24. Does the relevant national regulator need to approve the data transfer agreement?

The Israeli Registrar of Databases does not need to approve the data transfer agreement.

ENFORCEMENT AND SANCTIONS

25. What are the enforcement powers of the national regulator?

The Registrar of Databases (*Registrar*) is the regulatory authority under the Protection of Privacy Law 5741-1981 (*PPL*).

The Registrar operates within the Israeli Law, Information, and Technology Authority at the Ministry of Justice. The Registrar has investigative and audit powers. Under the PPL, Registrar inspectors are authorized to:

- Conduct announced or unannounced audits at premises where databases are administered.
- Collect evidence.
- Seize computers.
- Impose administrative sanctions in several forms:
  - declarations of fault;
  - fines; and
  - suspension or revocation of database registration.

26. What are the sanctions and remedies for non-compliance with data protection laws?

The Protection of Privacy Law 5741-1981 (*PPL*) provides for the following penalties:

- Administrative fines for violations of the PPL's data protection regime in amounts ranging from 10,000 NIS to 25,000 NIS. Continuous violations following a cease and desist letter from the Registrar of Databases can increase the fine by an additional 10% for each day during which the violation continues.
- Up to one year in prison for:
  - the strict liability offense of using an unregistered database whose registration is compulsory under the PPL;
  - using a database for purposes other than its registered purpose;
  - failing to provide data subjects access to their data and to allow them to correct or delete their personal data;
  - failure of a holder of databases owned by others to make sure that access to each database is only granted to those explicitly authorized in a written agreement between the holder and the owner of each database; and
  - non-compliance with the requirement to appoint an information security officer.

Violation of the PPL's privacy or data protection regime is also civil tort. Available remedies include:

- Actual damages for proven injury or harm.
- Injunctions.
- Statutory damages in an amount up to 100,000 NIS, which only applies to violation of the PPL's privacy regime.

Most forms of invasion of privacy under the PPL's privacy regime also give rise to a criminal offense punishable by up to five years in prison.

© 2017 Thomson Reuters. All rights reserved.

REGULATOR DETAILS

THE ISRAELI LAW, INFORMATION AND TECHNOLOGY AUTHORITY (ILITA) (ומידע טכנולוגיה ,למשפט הרשות – ט"רמו)

W www.justice.gov.il/En/Units/ILITA/Pages/default.aspx

Main areas of responsibility:

The ILITA is a unit within the Ministry of Justice. It houses three regulatory powers:

- The Registrar of Databases (the Israeli privacy regulator).
- The Registrar of Certification Authorities, pursuant to the Israeli electronic (digital) signature regime.
- The Registrar of Credit Data Service, pursuant to Israeli legislation governing the collection and dissemination of data regarding the creditworthiness of individuals and sole proprietors.

The ILITA is vested with regulatory oversight, investigative, audit, and enforcement powers.

ONLINE RESOURCES

W http://main.knesset.gov.il/Activity/Legislation/Laws/Pages/lawhome.aspx

Description. This is the website of the Knesset, the Israeli Parliament. It is in Hebrew and maintained by the Israeli Parliament. Provides non-consolidated, official Hebrew texts of statutes.

W www.justice.gov.il/Units/ilita/Pages/default.aspx

Description. The Israeli privacy regulator's website in Hebrew. Provides access to press releases, guidelines, annual reports, Q&As, descriptions of ongoing enforcement activities, and guidance on database registration.

W www.justice.gov.il/En/Units/ILITA/Pages/default.aspx

Description. The Israeli privacy regulator's English website. Provides out-of-date and non-official English translation of the Israeli Protection of Privacy Law, an unofficial English translation of the data transfer regulations, and several other guidance documents in English.

W www.wipo.int/edocs/lexdocs/laws/en/il/il084en.pdf

Description. Up-to-date but non-official English translation of the Israeli Protection of Privacy Law, prepared by WIPO.

CONTRIBUTOR PROFILES

HAIM RAVIA, SENIOR PARTNER, CHAIR OF THE INTERNET, CYBER AND COPYRIGHT PRACTICE GROUP

Pearl Cohen Zedek Latzer Baratz

T +972-9-972-8083

F +972-9-972-8001

E HRavia@PearlCohen.com

W www.pearlcohen.com; www.law.co.il

Professional qualifications. Attorney, Israel, 1990; Mediator, Israel 2002

Areas of practice. Data protection; cyber and privacy; computer and internet law; IT contracts; copyright; electronic signatures; open-source software.

Representative matters

- Counselling a multinational technology corporation on Israeli privacy and data protection law applicable to collecting employee-created emails for use in U.S. litigation.
- Counselling a major multinational corporation on workplace privacy and whistle-blower hotline matters applicable to its Israeli subsidiary.
- Advising a major Israeli financial institution on the legal restrictions under data protection laws applicable to the migration of its data operations to an outsourced cloud solution.
- Counselling a prominent Israeli public institute on the privacy law implications of its proposed project to digitize its voluminous physical archives in order to then make them publically accessible online.

Languages. English and Hebrew

Professional associations/memberships. The Israeli Chamber of Mediators.

Publications

- *Israel, in THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 190 (2d ed., Alan Charles Raul ed., 2015).*
- *Has written columns on Internet law for Globes (a major Israeli financial newspaper), the Israel Bar Association Magazine and other publications.*
- *Operates Israel's first legal website (*www.law.co.il*) and publishes commentaries on Lexology.*

© 2017 Thomson Reuters. All rights reserved.

DOTAN HAMMER, SENIOR ASSOCIATE IN THE INTERNET, CYBER AND COPYRIGHT PRACTICE GROUP

Pearl Cohen Zedek Latzer Baratz

T +972-9-972-8242

F +972-9-972-8001

E DHammer@PearlCohen.com

W www.pearlcohen.com; www.law.co.il

Professional qualifications. Attorney at law, Israel, 2012

Areas of practice. Data protection; Cyber and privacy; computer and Internet law; IT contracts; copyright; electronic signatures; open-source software.

Non-professional qualifications. B.A., Computer Science, Open University of Israel

Languages. English and Hebrew

Publications

- *Israel, in THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 190 (2d ed., Alan Charles Raul ed., 2015).*
- *Contributes to Israel's first legal website (*www.law.co.il*), Lexology, and other online publications.*

ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at **legalsolutions.com/practical-law**. For more information or to schedule training, call **1-800-733-2889** or e-mail **referenceattorneys@tr.com.**

04-17

© 2017 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (http://static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (https://a.next.westlaw.com/Privacy).