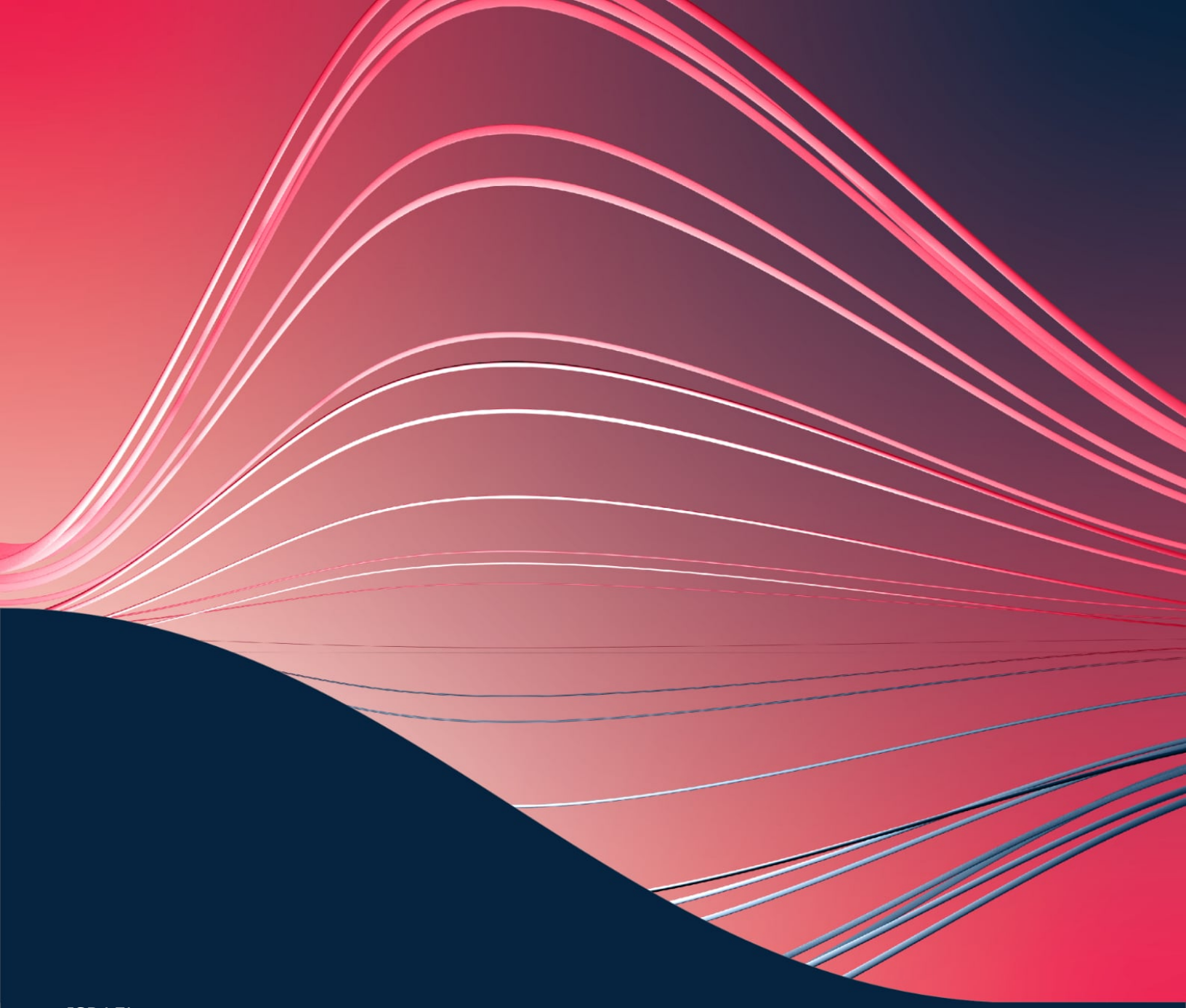


ISRAEL

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. As we step into 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

Europe

Established data protection laws in Europe continue to evolve through active regulatory guidance and enforcement action. In the United Kingdom, the UK government has proposed reforms to data protection and e-privacy laws through the new Data (Use and Access) Bill ("**DUAB**"). The DUAB follows the previous government's unsuccessful attempts to reform these laws post-Brexit, which led to the abandonment of the Data Protection and Digital Information (No.2) Bill ("**DPDI Bill**"), in the run-up to the general election. Although the DUAB comes with some bold statements from the government that it will *"unlock the power of data to grow the economy and improve people's lives"*, the proposals represent incremental reform, rather than radical change.

United States

In the United States, legislation on the federal and in particular state level continues to evolve at a rapid pace. Currently, the US has fourteen states with comprehensive data privacy laws in effect and six state laws will take effect in 2025 and early 2026. Additionally, at the federal level, the new administration has signaled a shift in enforcement priorities concerning data privacy. Notably, there is a renewed focus on the regulation of artificial intelligence (AI), with an emphasis on steering away from regulation and promoting innovation. This includes the revocation of previous executive orders related to AI and the implementation of new directives to guide AI development and use.

In the realm of children's privacy, many of the new administration's supporters in Congress have indicated a desire to make the protection of children on social media a top priority, and new leadership at the Federal Trade Commission (FTC) appears aligned on this goal, albeit with a willingness to take another look at the recently adopted amendments to the Children's Online Privacy Protection Act (COPPA) Rule. Health data

privacy remains a critical concern, with a handful of states following Washington state's lead in enhancing or adopting health data privacy laws. On the international data transfer front, Executive Order (E.O.) 14117 " Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" as supplemented by the DOJ's final Rule will impact companies transferring data into certain jurisdictions, such as China, Iran and Russia. Another area of focus for companies with an EU presence will be the Trump administration's approach to the Privacy and Civil Liberties Oversight Board, as it is a critical pillar of the EU/UK/Swiss-US Data Privacy Framework.

Asia, the Middle East, and Africa

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia, with new laws in India, Indonesia, Australia and Saudi Arabia, as well continued new data laws and regulations in China and Vietnam. The ever-evolving data laws, as well as the trend towards regulating broader data categories (beyond personal data), in these regions continue to raise compliance challenges for multi-national businesses.

Emerging trends in data governance

Unlocking data, regulating the relentless advance of AI, creating fairer digital markets and safeguarding critical infrastructure against the ever growing cyber threat, continue to impact and overlap with the world of data protection and privacy. Perhaps most notably, the EU have introduced a raft of new laws forming part of its ambitious digital decade, which will bring huge change to businesses operating within the EU. With the rapid adoption of artificial intelligence enabled solutions and functionality, data protection supervisory authorities have been closely scrutinising the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate date protection compliance into the core design and functionality of their AI systems. In the midst of this, the privacy community found itself at the centre of an emerging debate about the concept of 'AI governance'. This is not a surprising development – AI systems are creatures of data and the principle-based framework for the lawful use of personal data that sits at the heart of data protection law offers a strong starting point for considering how to approach the safe and ethical use of AI. As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services to enrich data. Whilst privacy professionals cannot tackle the AI challenge alone, expect them to continue to be on the front lines throughout 2025 and beyond.

Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

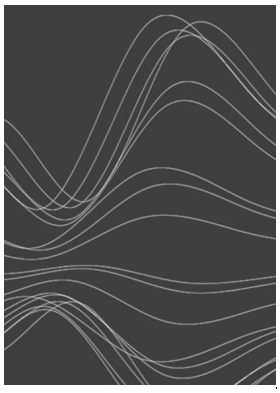
Africa key contact

Monique Jefferson
Director
monique.jefferson@dlapiper.com
Full bio

Americas key contact

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

Asia Pacific key contact



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

Europe key contacts

Andrew Dyson
Partner
andrew.dyson@dlapiper.com
Full bio

Ewa Kurowska-Tober
Partner
Head of Intellectual Property and Technology, Poland
ewa.kurowska-tober@dlapiper.com
Full bio

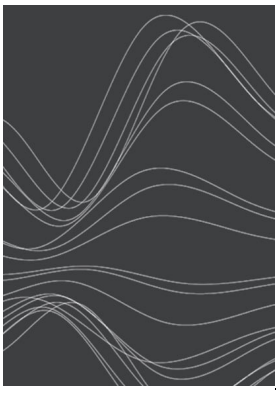
John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Middle East key contact

Rami Zayat
Partner
rami.zayat@dlapiper.com
Full bio

Editors

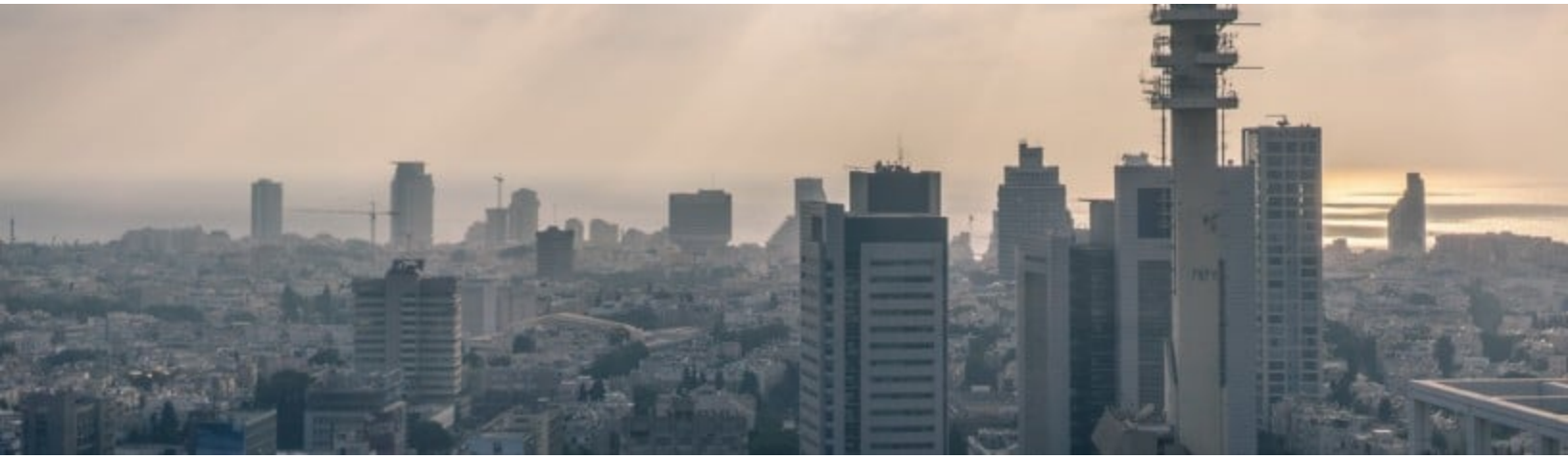
Kate Lucente
Partner
kate.lucente@us.dlapiper.com
Full bio



Lea Lurquin
Associate
lea.lurquin@us.dlapiper.com
Full bio

Israel

LAST MODIFIED 25 DECEMBER 2024



Data protection laws

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). On August 5, 2024, the Israel Knesset approved PPL (Amendment No. 13), 5774-2024 ("**Amendment 13**") which shall come into effect on August 14, 2025.

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 currently 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] Amendment 13 replaced the definition of Sensitive Data with the term "Especially Sensitive Data" which is broadly defined and includes various types of Personal Data, such as information about a person's intimate life, medical information, sexual orientation, genetic data, biometric identifiers, ethnicity, criminal records, political opinions, religious beliefs, location data, salary and financial activity, personality assessments and personal data subject to a statutory confidentiality obligation.

Footnotes

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 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 that currently 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.

Amendment 13 limited the abovementioned registration requirements to apply to the extent one of the following conditions are met:

- Databases containing Personal Data about more than 10,000 data subjects and its main purpose is the collection of Personal Data for the purpose of transferring to third parties, either for business purposes or in exchange for compensation (including direct marketing services); or
- The controller of the database is a Public Body (as defined in Section 23 of the PPL), unless the database contains Personal Data only with respect to the employees of the Public Body.

Amendment 13 also added a notification requirement to the IPA in the event that a database that does not require registration contains Especially Sensitive Data in respect of more than 100,0000 data subjects.

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.

Footnotes

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 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 Security 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 Security 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 Security 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 / controller, 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 / controller and its supervisor.

Amendment 13 added a requirement to appoint a Data Protection Officer under the following circumstances: (i) controller is a Public Body as defined in Section 23 of the PPL, (ii) controller of a database with a main purpose of collecting Personal Data in order to transfer it to a third party (data brokers) and the database contains Personal Data of more than 10,000 data subjects, (iii) controllers and processors whose main activities include processing which in light of its nature, scope or purpose require regular and systematic monitoring of data subjects on a Large Scale (as defined in Amendment 13), or (iv) controllers and processors of databases that include Especially Sensitive Data on a Large Scale (as defined in Amendment 13). Large Scale will be determined by, among other things, the number of data subjects whose Personal Data is processed, their proportion within a specific population, the scope and volume of the Personal Data, the variety of data types processed, the duration and frequency of the processing activities, the retention period of the Personal Data, and the geographical area where the processing occurs. The DPO must have the required expertise and abilities to carry out their responsibilities effectively, including in-depth knowledge in privacy protection laws, adequate understanding of technology and security information and the company's operations and goals. The DPO will not take on any additional roles nor be subordinate to any official within the body where they hold their position, or in any other body, if such a role or subordination could create a conflict of interest that would interfere with the performance of their duties. The DPO will report directly to the CEO or another senior executive and may be external to the company. The DPO will advise the company's management and staff on privacy-related issues, design and oversee a privacy training program, establish and maintain ongoing compliance monitoring, address data subject inquiries, and serve as the point of contact with the IPA.

Collection and 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;
- the purpose(s) of use of the data;
- the consequences of refusing the collection and processing of the data (added in Amendment 13);
- controller's name and contact information (added in Amendment 13); and
- the data subject's right to access and rectify the data (added in Amendment 13).

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 February 28, 2024, the IPA published Guideline: Collection and Use of Biometric Information in the Workplace. Employers who use biometric systems to monitor employees' attendance can do so provided that they appropriately address and respect the employees’ right to privacy, in accordance with notice and consent requirements and adherence to proportionality, transparency, purpose limitation, security and data minimization principles.

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 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 January 8, 2024, the Knesset committee approved in its second and third reading the 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.

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 July 11, 2024, the IPA published Recommendations: Use of Tracking Tags, which includes recommendations for safe use of tracking tags while maintaining user privacy.

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 February 22, 2024, the IPA published: Recommendations for the Public while Using Charging Stations for Electric Vehicles, including recommendations for safe and balanced use of electric vehicles charging stations, while preserving the privacy of the users.

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 March 5, 2024, the IPA published Policy: Protection of Patients' Privacy in the Transmission of Medical Information Through Digital Means which includes recommendations for organizations, medical professionals, and healthcare institutions on transfer of medical information such as: limiting the use of non-specialized software for transmitting medical information, omitting medical data, ensuring proper security, and establishing a clear organizational policy.

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).

On March 17, 2024, the IPA published Opinion: Collection of ID Numbers and Photographs of IDs, which outlines how and when a company may collect ID Numbers and photographs of IDs from consumers.

On September 18, 2024, the IPA published Guidance: Guiding Principles in Emergency Situations, which empathizes the balance between urgency and efficient actions during an emergency (e.g. war, natural disasters (earthquakes, floods), terrorist events on a large scale, and epidemics) and the obligation to protect privacy rights and infringement thereof. The IPA states that there is an obligation to respect privacy rights and to avoid unnecessary violations whenever possible.

On September 24, 2024, the IPA published Recommendations: Use of Tourist Applications, which include recommendations for proper conduct when using travel applications.

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.

On 15 January 2024 the EU Commission has issued a "Report from the Commission to the European Parliament and the Council on the First Review of the Functioning of the Adequacy Decisions Adopted Pursuant to Article 25(6) Of Directive 95/46/EC", in which it was announced that Israel's adequacy status from January 31, 2011, had been renewed.

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.

Footnotes

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, including having in place a policy which defines inter alia supervision processes, controls, and effective compliance.

On May 9, 2024, the IPA published Opinion: Conducting Risk Assessments and Penetration Tests on Information Systems, which recommends organizations and Personal Data repositories to conduct voluntary risk assessments and penetration tests (not only in respect of a high security level database which according to the Data Security Regs such testing is mandatory).

On September 29, 2024, the IPA published Guidance: Implementation of Section 10 of the Data Security Regs - Keeping Records and Logs, which clarifies the manner of implementation of the obligations to manage an automatic documentation mechanism by keeping records and logs in databases classified as having a medium or high level of security.

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.

Amendment 13 establishes the possibility for controllers or processors of databases to request IPA preliminary opinions regarding the compliance with the PPL of their databases or data processing practices with the law. Amendment 13 provides IPA with the ability to conduct criminal investigations and to impose monetary sanctions. In addition, Amendment 13 expands the grounds for granting statutory damages without the need to prove actual damages including in the event of failure to register a database, failure to meet the disclosure requirements, failure to comply with a request to access or correct information, etc.

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.

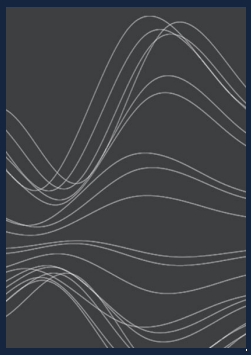
The PPL governs information "about a person", as such depending upon the circumstances at hand, any nonidentifiable and anonymous information (which cannot be reidentified) may reasonably be interpreted as falling outside the confines of the PPL limitations.

Data protection lawyers

Sharon Aloni
Partner
Goldfarb Seligman & Co.
sharon.aloni@goldfarb.com
View bio

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com