DATA PROTECTION LAWS OF THE WORLD

Israel vs Germany

DLA PIPER

ISRAEL

Last modified 22 December 2023

LAW

The laws that govern the right to privacy in Israel are the Basic Law: Human Dignity and Liberty, 5752 -1992; the Protection of Privacy Law, 5741-1981 and the regulations promulgated thereunder (the 'PPL') and the guidelines of the Israel Privacy Authority (as defined below).

GERMANY

Last modified 19 January 2024

LAW

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two-year transition period, became directly applicable law in all Member States of the European Union on May 25, 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

Germany has adjusted the German legal framework to the GDPR by passing the new German Federal Data Protection Act (*Bundesdatenschutzgesetz* – "**BDSG**"). The BDSG came into force together with the GDPR on May 25, 2018. The purpose of the BDSG is

especially to make use of the numerous opening clauses under the GDPR which enable Member States to specify or even restrict the data processing requirements under the GDPR. Part 3 of the BDSG implements the Law Enforcement Directive (EU) 2016/680.

Find the English version here.

In addition to the BDSG, there exist a number of data protection rules in area-specific laws, for example those regulating financial trade or the energy sector. As of 1 December 2021, the Telecommunications-Telemedia-Data Protection Act (*Telekommunikation-Telemedien-Datenschutzgesetz* – "**TTDSG**") provides data protection regulations for telecommunication and telemedia providers, which are intended to eliminate a long-standing legal uncertainty about the applicability of the data protection regulations of the German Telecommunications Act (*Telekommunikationsgesetz* – "**TKG**") and the German Telemedia Act (*Telemediengesetz* – "**TMG**") in interaction with the GDPR. The TTDSG also transposes the “cookie consent” requirement under Article 5 (3) ePrivacy Directive into German law.

DEFINITIONS

Definition of personal data

Personal Data, as defined under the PPL, means: data regarding the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.

Definition of sensitive personal data

Sensitive Data, as defined under the PPL, means: data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person; and other information if designated as such by the Minister of Justice with the approval of the Constitution, Law and Justice Committee of the Knesset. No such determination has been made to date.[1]

1: On July 23, 2020, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Definitions and

DEFINITIONS

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "identifiable" – if the natural person can be identified using “*all means reasonably likely to be used*” (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

Limiting Registration Obligations) 5782- 2021. The draft bill proposes to revise defined terms under the PPL to align with the definition in the GDPR, such as definition of: personal data, sensitive data, processing, owner of a database, holder of a database and other. In addition, the draft bill attempts to limit database registration requirements to apply to certain categories of databases containing information of 100,000 data subject or more. The draft bill has yet to be placed on the table of the Israel Knesset for its first reading. Furthermore, the draft bill expands the administrative enforcement of the IPA. On May 18, 2021, the Israeli Ministry of Justice published two draft bills proposing to amend the PPL (Appointment of an Official Representative) 5782-2021 and the PPL (Minor's Privacy) 5782-2021. On July 26, 2021, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Limitation Period) 5721-2021 to extend the limitation period by which a civil claim may be filed under the PPL from a period of two years to a period of seven years, in accordance with the Statute of Limitations Law 5718-1958. All the foregoing draft bills have been placed on the table of the Israel Knesset and for their preliminary discussion. On January 5, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Amendment Number 14) 5782-2021. The draft bill proposes to increase the supervisory and enforcement capabilities of the IPA (such as impose financial sanctions for violating the provisions of the law concerning the management of databases up to an amount of NIS 3.2 million), to reduce the obligation to register databases as well as to adapt the defined terms under the Israel Protection of Privacy Law to the technological developments and modern privacy legislation. The draft bill has been approved in its first reading of the Israel Knesset and is in preparation for the second and third reading in the Knesset committee. On January 31, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Strengthening the Right to Privacy and its Protection) 5782-2021. The draft bill proposes additional rights of data subjects to control their personal information. In addition, the draft bill includes further strengthening of the enforcement powers of the IPA, in particular with regards to enforcement on an international level. The draft has been set on the Knesset's table for its first reading. On January 31, 2022, the Israeli Ministry of Justice published a draft bill proposing to amend the PPL (Deletion from Databases), 5782-2022. The draft bill proposes to add requirements to the notification obligations to data subjects, prior to collecting personal information (Section 11 of PPL), such as adding an obligation to indicate when a renewed authorization to hold the personal information will be requested and

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

The definitions are the same as in Article 4 GDPR. Beyond that, the BDSG contains further definitions for 'public bodies of the Federation', 'public bodies of the Länder' and 'private bodies' in Section 2 BDSG. The TTDSG contains definitions for types of data that are specifically related to the provision of telecommunications and telemedia services (so-called inventory data and usage data).

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.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, the CNIL in France or the Garante in Italy). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the Regulation.

The GDPR creates the concept of "**lead supervisory authority**". Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by and answer to the supervisory authority for their main or single establishment, the so-called "lead supervisory authority" (Article 56(1)).

However, the lead supervisory authority is required to cooperate with all other "concerned" authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

Germany does not have one central supervisory authority for data protection law but authorities in each of the sixteen German federal states (*Länder*) that are competent for the public and the private sector in the respective state. In addition, there are different supervisory authorities for private broadcasters as well as for public broadcasters and several supervisory authorities for religious communities.

The German Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für Datenschutz und Informationsfreiheit* – "**BfDI**") is the supervisory authority for all federal public bodies as well as for certain social security institutions; it also supervises telecommunications and postal service providers, insofar as they provide telecommunications or postal services. The BfDI represents Germany in the European Data Protection Board. To ensure that all the supervisory authorities have the same approach, a committee consisting of members of all authorities for the public and the private sector has been established – the 'Data Protection Conference' (*Datenschutzkonferenz* "**DSK**"). The coordination mechanism between the German supervisory authorities for data protection law mirrors the consistency mechanism under the GDPR.

A list with the contact details and websites of most of the supervisory authorities can be found here.

REGISTRATION

Subject to certain exceptions, database registration is required to the extent one of the following conditions are met[1]:

- the database contains information in respect of more than 10,000 data subjects;
- the database contains sensitive information;
- the database includes information on persons, and the information was not provided by them, on their behalf or with their consent;
- the database belongs to a public entity; or
- the database is used for direct marketing services.

A database is defined under the PPL as a collection of data, stored by magnetic or optic means and intended for

REGISTRATION

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in

computer processing, consequently excluding noncomputerized collections.

In 2005, the Ministry of Justice set up a committee generally known as the 'Schoffman Committee' which recommended relaxing registration of 'ordinary' databases and focusing on specific categories of information (e.g. medical data, criminal records or information about a person's political or religious beliefs). However, to date, the Schoffman Committee recommendations have not crystallized into binding legislation.

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

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

the GDPR by rigorous demands for internal accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out

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

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

DATA PROTECTION OFFICERS

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

- a possessor of five databases that require registration;
- a public body as defined in Section 23 to the PPL; or
- a bank, an insurance company or a company engaging in rating or evaluating credit.

Failure to nominate a Data Protection Officer when required to do so may result in criminal sanctions, within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

There is no general requirement in Germany for controllers or processors to register their processing activities with the competent supervisory authority for data protection law; however, a register of data protection officers (DPOs) is maintained.

DATA PROTECTION OFFICERS

Each controller or processor is required to appoint a data protection officer (DPO) if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single DPO with responsibility for multiple legal entities (Article

including administrative fines. The PPL does not require that the Data Protection Officer should be an Israeli citizen or resident.

In the event that a data protection officer was appointed pursuant to the PPL, the Israel Protection of Privacy Regulations (Data Security), 5777-2017 ('Data Security Regs') require that the officer be directly subordinate to the database manager, or to the manager of the entity that owns or holds the database. In addition, the Data Security Regs prohibit the officer from being in a conflict of interest and require the officer to establish data security protocols and ongoing plans to review compliance with the Data Security Regs. The officer must present findings from such review to the database manager and its supervisor.

37(2)), provided that the DPO is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single DPO).

DPOs must have "expert knowledge" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

The threshold to designate a DPO is much lower in the BDSG. The controller and processor has to designate a DPO if they constantly employ as a rule at least 20 persons dealing with the processing of personal data by automated means, Section 38 (1) sentence 1 BDSG. The meaning of ‘automated processing’ is interpreted broadly by the German Authorities. It basically covers every employee who works with a computer.

If the threshold of 20 persons is not reached, Section 38 (1) sentence 2 BDSG regulates, that a DPO has to be designated in case the controller

or processor undertakes processing subject to a data protection impact assessment pursuant to Article 35 GDPR, or if they commercially process personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research.

A dismissal protection for the DPO is provided in Section 38 (2) in conjunction with Section 6 (4) BDSG. Where the controller or processor is obliged to appoint a DPO, the dismissal of a DPO, who is an employee, is only permitted in case there are facts which give the employing entity just cause to terminate without notice. After the activity as DPO has ended, a mandatory DPO who is an employee may not be terminated for a year following the end of appointment, unless the employing entity has just cause to terminate without notice.

Additionally, Section 38 (2) in conjunction with Section 6 (5) and (6) BDSG stipulates that the DPO shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified, unless he / she is released from this obligation by the data subject. Also, the DPO has the right to refuse to give evidence under certain conditions.

Moreover, the German supervisory authorities expect that the DPO speaks the language of the competent authority and the data subjects, i.e. German, or at least that instant translation is ensured.

The supervisory authorities maintain a register of DPOs. No fee is charged for registering or updating the details of a DPO.

COLLECTION & PROCESSING

The collection, processing or use of Personal Data is permitted subject to obtaining the informed consent of the data subjects. Such consent should adhere to purpose, proportionality and transparency limitations. As such, consent should be obtained for specific purposes of use, the processing and use of Personal Data should be proportionate to those purposes, and data subjects should have the right to inspect and correct their personal information. The data subject's consent must be reobtained for any change in the purpose of use.

COLLECTION & PROCESSING

Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be (Article 5):

- processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle");

Any request for consent from a data subject to have his or her Personal Data stored and used within a database must be accompanied by a notice indicating:

- whether there is a legal requirement to provide the information;
- the purpose for which the information is requested;
- the recipients of the data; and
- the purpose(s) of use of the data.

Retaining outsourcing services for the processing of personally identifiable information is subject to the IPA's Guidelines on the Use of Outsourcing Services of Processing Personal Information (Guideline 2/2011) dated 10 June 2012 ('Outsourcing Guidelines'). The Outsourcing Guidelines include, inter olio, factors to be taken into consideration when deciding to use outsourcing services, specific provisions to be included within the data transfer agreement and data security requirements. Processing of personally identifiable information in certain sectors is subject to additional outsourcing requirements.

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

Entities subject to separate outsourcing guidelines are for example entities supervised by the Commissioner of the Capital Market, Insurance and Savings and entities supervised by the Banking Supervision Department of the Bank of Israel. On 10 September 2014, the Banking Supervision Department of the Bank of Israel issued draft guidelines regarding risk management in cloud computing services used by Israeli banking corporations. Among other various restrictions, the draft guidelines set forth an obligation on supervised entities to receive the approval of the Supervisor of Banks prior to using cloud computing services. The general issue of privacy consideration in the use of surveillance cameras is governed by the IPA Use of Surveillance Cameras and the Footage Obtained Therein Guidelines (no. 4/2012). In 2017, the IPA published Use of Surveillance Cameras in the Workplace and in Working Relationships Guidelines (no. 5/17) specifically referring to the use of surveillance cameras in the workplace. The guidelines state that the employer's prerogative to use surveillance means in the workplace is subject to fulfillment of principals such as legitimacy, transparency, proportionality, good faith and fairness. These principles apply also to businesses required by law enforcement to place surveillance cameras on their premises. The guidelines specify the manner in which these principles should be implemented, derivative requirements and possible implications.

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle");
- adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- accurate and where necessary kept up-to-date (the "accuracy principle");
- kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle"); and
- processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle").

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance perhaps years after a particular decision relating to processing personal data was taken. Record-keeping, audit and appropriate governance will all form a key role in achieving accountability.

Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known as lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- with the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time);
- where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract;
- where necessary to comply with a legal obligation (of the EU) to which the controller is subject;
- where necessary to protect the vital interests of the data subject or another person (generally recognized as being limited to 'life or death' scenarios, such as medical emergencies);
- where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the

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

controller; or

- where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks).

Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- with the explicit consent of the data subject;
- where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement;
- where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent;
- in limited circumstances by certain not-for-profit bodies;
- where processing relates to the personal data which are manifestly made public by the data subject;
- where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity;
- where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards;
- where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services;
- where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices; or
- where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1).

hours Personal Data collection, and the duration for which the information will be retained.

On May 22, 2023, the IPA published Publication: Privacy Related Aspects of Monitoring Remote Working Employees, which includes certain standards required for employers that monitor their employees working remotely in order to avoid breach of their privacy rights (including without limitation compliance with proportionality and legitimacy standards such as limiting surveillance solely to work hours; employers must inform their employees that they are using technological means to monitor their behavior when working remotely, including the purpose for which the monitoring is done).

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

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

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

On July 23, 2020, the Special Authorities to Combat the Novel Corona Virus (Temporary Order) 5780 – 2020 came into effect (by virtue of the Israel Government's authority under Section 39 of the Basic Law: The Government). Under the Temporary Order, and the authorities granted to the Israel General Security Service ('GSS') by the General Security Service Authorization Law 5762-2002, the Government may establish new regulations which potentially broaden Israel Government authorities / GSS rights in respect of collection and processing Personal Data, such as: the Emergency Regulations (General Security Service Authorization to Assist in the National Effort to Reduce the Spread of the Novel Corona Virus), 5780- 2020 which authorized the GSS to perform surveillance on Israel citizens to reduce the spread of the Corona Virus; Emergency Regulations (Location Data), 5780-2020 were established amending the Criminal Procedure Law (Enforcement Powers – Communication Data) 5768- 2007 authorizing the Israel Police to preform cell

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law (Article 10).

Processing for a Secondary Purpose

Increasingly, organisations wish to 're-purpose' personal data - *ie,* use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- any link between the original purpose and the new purpose
- the context in which the data have been collected
- the nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- the possible consequences of the new processing for the data subjects
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, *ie,* the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The

phone surveillance (i.e. receiving the location of a cell phone from a cellular operator) of a Corona virus patient without a court order; and the Emergency Regulation (General Security Service to assist in National Effort to Reduce Spread of Omicron Strain of Novel Corona Virus), 5782- 2021 that permit the GSS to perform surveillance of Israel citizens. The Temporary Order has been extended until February 15, 2024, in order to maintain a legal infrastructure that enables taking actions under the law to reduce the spread of the coronavirus and reduce harm to public health.

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

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

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

On June 6, 2023, Inclusion of Biometric Identification Means and Biometric Identification

presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- the identity and contact details of the controller;
- the data protection officer's contact details (if there is one);
- both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing;
- the recipients or categories of recipients of the personal data;
- details of international transfers;
- the period for which personal data will be stored or, if that is not possible, the criteria used to determine this;
- the existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability;
- where applicable, the right to withdraw consent, and the right to complain to supervisory authorities;
- the consequences of failing to provide data necessary to enter into a contract;
- the existence of any automated decision making and profiling and the consequences for the data subject; and
- in addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information.

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

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

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

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

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

On December 11, 2023, the government published Memorandum of Law: Israel Security Agency (Amendment No....), 2023 open to comments by the public, which purpose is to regulate certain aspects including cyber and computers and to grant GSS rights to receive, collect and transmit information, including from databases, subject to certain approvals, supervision and control mechanisms. Which is in addition to the publication by the Israeli Ministry

Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when the European Union’s highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

of Justice published on February 28, 2021 the draft bill Memorandum: "The Cyber Defense Law and the National Cyber System (Authorities for the Purpose of Strengthening Protection) (Temporary Order), 5781-2021", which states that the National Cyber System and the GSS will be permitted to give instructions to private and public organizations in Israel on how to prepare for and defend against a cyber-attack and addresses compliance issues.

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

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

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

Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest. Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

The right not to be subject to automated decision making, including profiling (Article 22)

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

a. necessary for entering into or performing a contract;
b. authorized by EU or Member State law; or
c. the data subject has given their explicit (i.e. opt-in) consent.

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

The BDSG has additional rules regarding processing of special categories of personal data. Contrary to Article 9 (1) GDPR, processing of such data is permitted by public and private bodies in some cases which are based on the exceptions in Article 9 (2) GDPR, see Section 22 (1), 26 (3) BDSG. Also, Section 24 BDSG determines cases in which controllers are permitted to process data for a purpose other than the one for which the data were collected.

Section 4 BDSG provides a special rule for video surveillance of publicly accessible areas. According to the German data protection supervisory authorities as well as the German Federal Administrative Court (*Bundesverwaltungsgericht* – "**BVerwG**") and the near unanimous opinion in German legal literature, the provision is not compliant with the GDPR insofar as it regulates surveillance by private bodies (Section 4

(1) Nos. 2, 3 BDSG). This is based on the argument that the GDPR does not contain any opening clause on which these deviations from Article 6 (1) GDPR could be based.

Furthermore, the BDSG provides special rules regarding processing for employment-related purposes in Section 26 BDSG. The German legislator has made very broad use of the opening clause in Article 88 (1) GDPR and has basically established a specific employee data protection regime, that mostly only repeats the general legal bases of performance of contract respectively “*carrying out the obligations and exercising specific rights… in the field of employment and social security and social protection law*” (Art. 9(2)(b) GDPR). Due to this, the European Court of Justice ruled that a provision in German state data protection law (which applies to the public sector) that corresponds with the “performance of the employment contract” legal basis in Section 26 BDSG is invalid (Judgment of the CJEU in Case C-34/21). This is because the law failed to establish specific provisions, although this is a requirement pursuant Article 88(1) GDPR for national legal bases. Due to this decision, it is widely assumed (including by the German supervisory authorities that (some) of the respective German legal bases for the processing of employee personal data in the BDSG are invalid.

Employers should therefore rely (alternatively or additionally) on the GDPR legal bases for the processing of employee and candidate personal data for the establishment or the performance of the employment contract (Article 6(1)(b) GDPR) respectively on Article 9(2)(b) GDPR. In particular when determining what is “necessary” for the performance of the employment contract, employers also need to comply with the case law of the German Federal Labour Court (*Bundesarbeitsgericht* – "**BAG**").

In addition, there is a legal basis specifically for the investigation of criminal offences against employees which likely is still valid.

Furthermore, processing of employee personal data for purposes that are not specifically related to employment as such can still be based on Article 6 (1) GDPR. In particular, controllers that

are part of a group of companies may be able to base transfers of data within the group for internal administrative purposes on their legitimate interests in accordance with to Article 6 (1) f) (as stated by Recital 48 of the GDPR).

The processing of personal data in the context of the provision of telecommunication services is subject to Section 9 et seqq. TTDSG. Furthermore, both the content of telecommunications and its detailed circumstances, in particular the fact whether someone is or was involved in a telecommunications process, is subject to the secrecy of telecommunications, Section 3 TTDSG. Violations of the secrecy of telecommunications constitutes a criminal offence under the German Criminal Code (*Strafgesetzbuch* – "**StGB** ").

The processing of personal data in the context of the provision of telemedia (like for example a website or a social network) is subject to specific limitations contained in Section 19 et seqq. TTDSG. There are, inter alia, specific requirements regarding the provision of inventory data, passwords or usage data to public authorities in Section 22 et seqq. TTDSG.

The following German specific rules for the processing of personal data in the employment context likely are still valid:

- Employees’ personal data may be processed to detect criminal offenses only if there is a documented reason to believe the data subject has committed such an offense while employed, the processing of such data is necessary to investigate the offense and is not outweighed by the data subject’s legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason (Section 26 (1) sentence 2 BDSG) (this blocks investigation based on legitimate interests pursuant Article 6(1) f GDPR);
- The processing is based on a works council agreement which complies with the requirements set out Article 88 (2) GDPR (Section 26 (4) BDSG);
- The processing is based on the employee’s consent in written or

electronic form. A derogation from this form can apply if a different form is appropriate because of special circumstances (but this derogation will rarely apply in practice). Moreover, the utilization of consent as basis for the processing is particularly problematic in Germany as Section 26 (2) BDSG stipulates requirements in addition to Article 7 GDPR. If personal data of employees are processed on the basis of consent, then the employee’s level of dependence in the employment relationship and the circumstances under which consent was given shall be taken into account in assessing whether such consent was freely given. Consent may be freely given in particular if it is associated with a legal or economic advantage for the employee, or if the employer and employee are pursuing the same interests. The German data protection supervisory authorities interpret this provision in a way that employee consent cannot be used for processing of personal data which directly relates to the employment relationship, but only to supplementary services offered by the employer (e.g. private use of company cars or IT equipment, occupational health management or birthday lists).

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;

TRANSFER

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)). Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand.

Transfers to third countries are also permitted where

- 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

appropriate safeguards have been provided by the controller or processor and on the condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules, standard contractual clauses, and the EU-US Privacy Shield Framework. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognized or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

protection with regard to automated processing of personal data.

Additionally, the transfer of databases is subject to the IPA Draft Guidelines No. 3/2017, which under certain circumstances, such as database recipient having a conflict of interest, might require opt-in consents of data subjects as a condition to transferring databases.

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

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

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

On September 14, 2023, the IPA published Manual: Contracting with Outsourcing Providers – Section 15 to the Data Security Regs,

The transfer of personal data to a third country or to supranational or intergovernmental bodies or international organisations in the context of activities not falling within the scope of the GDPR or the Law Enforcement Directive (EU) 2016/680 are also permitted if they are necessary for the performance of own tasks for imperative reasons of defence or for the performance of supranational or intergovernmental obligations of a federal public body in the field of crisis management or conflict prevention or for humanitarian measures.

For more information, please visit our Transfer - global data transfer methodology website.

which clarifies the manner in which companies shall contract with their outsourcing providers. The manual specifies issues to be included in the binding agreement between the company and the outsourcing provider, and it includes two appendices for use by the parties: an auxiliary questionnaire for checking the information security aspects of the outsourcing provider, and a proposed questionnaire to determine the method of performing the periodic control of the outsourcing provider.

1: Following the decision of the ECJ in Case C362/14 Maximillian Schrems v Data Protection Commissioner, IPA issued a statement on October 15, 2015, according to which US safe harbour certified entities would not fall under the foregoing condition, without derogating from all other conditions. Similarly following the decision of the CJEH in the Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, IPA issued a statement on September 29, 2020, according to which US privacy shield certified entities would not fall under the foregoing condition, without derogating from all other conditions.

SECURITY

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

Furthermore, the Data Security Regs add to the Outsourcing Guidelines, which in effect would expand the requirements applicable when outsourcing processing services, even prior to entering into a data transfer agreement between the database owner and the data recipient and the requirements to be included therein.

Failure to comply with the Data Security Regs will constitute a breach of the PPL, which may expose a non-compliant entity to criminal and civil liability, as well as to administrative fines.

SECURITY

Security

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However, the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

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.

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The BDSG has additional rules regarding the processing of special categories of personal data in Sec. 22 (2) BDSG. In case of processing of such data, appropriate and specific measures have to be taken to safeguard the interests of the data subject.

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, these measures may include in particular the following:

- technical and organizational measures to ensure that processing complies with the GDPR;
- measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered or removed;
- measures to increase awareness of staff involved in processing operations;
- designation of a data protection officer;
- restrictions on access to personal data within the controller and by processors;
- the pseudonymization of personal data;
- the encryption of personal data;
- measures to ensure the ability, confidentiality, integrity, availability and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
- specific rules of procedure to ensure compliance with this Act and with the GDPR in the event of transfer or

processing for other purposes.

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.

BREACH NOTIFICATION

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A "personal data breach" is a wide concept, defined as any "*breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*" (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a *high* risk to natural persons, the controller is also required to notify the affected data subjects without undue delay (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach (Article 33(2)).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3)).

Controllers are also required to keep a record of all data breaches (Article 33(5)) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

Personal data breaches should be notified to the competent supervisory authority. The German supervisory authorities generally make available specific web forms for notifications and some of them have published risk rating requirements for personal data breach notifications.

The German BDSG only contains slight changes and additions to the regulations in Article 33, 34 GDPR.

Section 29 (1) BDSG stipulates in addition to the

exception in Article 34 (3) GDPR, the obligation to inform the data subject of a personal data breach according to Article 34 GDPR shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party. By derogation from this, the data subject pursuant to Article 34 GDPR shall be informed if the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

According to Section 43 (4) BDSG, a notification pursuant to Article 33 GDPR or a communication pursuant to Article 34 (1) GDPR may be used in proceedings pursuant to the Act on Regulatory Offences (*Gesetz über Ordnungswidrigkeiten –* "**OWiG**") against the person required to provide a notification or a communication only with the consent of the person obligated to provide a notification or a communication.

ENFORCEMENT

IPA has the authority and obligation to supervise compliance and enforce the provisions of the PPL and appoint inspectors to carry out those activities.

Breach of the PPL may result in both civil and criminal sanctions, including administrative fines, 15 years of imprisonment, and the right to receive statutory damages under civil proceedings without the need to prove actual damages.

The current draft bill for the 13th Amendment of the PPL provides IPA with the ability to conduct criminal investigations and to impose monetary sanctions in the amount of up to NIS 3.2 million. The draft bill has passed its first reading, but has yet to pass the approval of the Knesset Constitution, Law and Justice Committee; thereafter it would need to also pass the second and third readings, in order to become a binding piece of legislation.

ENFORCEMENT

Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define ‘undertaking’ and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of ‘undertaking’. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some

circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.
The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects’ rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of “non-material”

damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

In October 2019 the German data protection authorities published guidelines for calculating administrative fines against ‘business undertakings’ under Article 83 GDPR. However, since the final version of the Guidelines 04/2022 on the calculation of administrative fines under the GDPR of the EDPB was adopted in May 2023, the German guidelines are no longer relevant.

Enforcement powers

There are no German specific enforcement powers except for the German Federal Commissioner for Data Protection and Freedom of Information (*Bundesbeauftragter für Datenschutz und Informationsfreiheit* – "**BfDI** ") competent for federal authorities and certain sectors (see Authority for details).

Administrative powers

German law provides for administrative fines of up to 50,000 EUR for the violation of German specific requirements for the processing of personal data in the context of consumer loans (Sections 30 and 43 BDSG).

Criminal offences

The BDSG provides for several offences which can result in prosecution of, imprisonment, and criminal penalties being imposed of / on individuals. The offences under the BDSG include:

- transferring personal data to a third party or otherwise making them accessible if done deliberately and without authorization for commercial purposes and with regard to the personal data of a large number of people which are not publicly accessible;
- processing without authorization, or fraudulently acquiring, personal data which are not publicly accessible if doing so in return for payment or with the intention of enriching oneself or someone else or harming someone.

Additionally other special laws provide for criminal offences (e.g. violations of the secrecy of telecommunications constitutes a criminal offence under the German Criminal Code (*Strafgesetzbuch* – StGB)).

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

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (*eg*, an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and *not* merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3)).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is likely to be replaced by a regulation (the so called ePrivacy Regulation), but it is currently uncertain when this is going to happen, as the European Commission has discarded its draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime,

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.

GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR. As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

In general, unsolicited electronic marketing requires prior opt-in consent. The opt-in requirement is waived under the ‘same service / product’ exemption. The exemption concerns marketing emails related to the same products/services as previously purchased from the sender by the user provided that:

- the user has been informed of the right to opt-out prior to the first marketing email
- the user did not opt-out, and
- the user is informed of the right to opt-out of any marketing email received. The exemption applies to electronic communication such as electronic text messages and email but does not apply with respect to communications sent by fax.

Direct marketing emails must not disguise or conceal the identity of the sender.

Like the GDPR, the German BDSG also does not provide for any specific provisions regarding marketing. The use of electronic communication for the purpose of direct marketing as currently regulated in ePrivacy Directive has been transposed into German law and is implemented in Section 7 of the German Act Against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb –* "**UWG**") As emphasized by the German Authorities (in their guidelines on direct marketing), processing of personal data for the purpose of marketing communication which is in breach of Section 7 UWG also constitutes a breach of the GDPR as it does not follow a legitimate purpose.

When using electronic communication for direct marketing, prior consent is generally required, cf. Section 7 (2) no. 1, 2 UWG, the standard for this being the so-called double opt-in process. According to Article 6 (1) a) GDPR as well as according to established German case law, data subjects must always give consent for a specific processing purpose. This means that the person

to be contacted needs to know (1) from whom (meaning which specific entity or entities), (2) for which specific products and services he / she will receive marketing offers and (3) by which means (e.g. email or telephone).

The German lawmaker has also transposed the ‘same service / product’ exemption into Section 7 UWG. Based on Section 7 (3) UWG, direct marketing can be based on the exemption if the following prerequisites are met:

- the recipients electronic mail address was obtained from the sender in connection with the sale of goods or services;
- the sender uses the address for direct advertising of his own similar goods or services (no cross-selling permitted);
- the recipient has not objected to this use; and
- the recipient is clearly and unequivocally advised, upon the collection of the address as well as each time it is used, that he or she can object to such use at any time, without costs arising by virtue thereof, other than transmission costs pursuant to the basic rates.

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.

ONLINE PRIVACY

The General Data Protection Regulation (GDPR) supersedes national data protection law unless there is an opening clause constituted under GDPR. Due to Article 95 GDPR this is the case for national data protection law that was created to implement the Directive on privacy and electronic communication (Directive 2002/58/EC; "ePrivacy Directive").

The German legislator created national data protection regulations for providers of telecommunication services and for providers of certain electronic information and communication services (e.g. website operators) within the TTDSG, which was adopted on 1 December 2021. The TTDSG aims to eliminate the legal uncertainties caused by the fact that special data protection provisions were previously regulated in two different laws, the TKG and the TMG, which were both not adapted to the GDPR. As a result, in the past German data protection authorities and courts sometimes disagreed on which of these provisions, if any, were applicable.

The TTDSG eliminates some provisions that were

deemed unapplicable and shifts the data protection regulations regarding telecommunication and telemedia into a single law, which stands alongside the GDPR and the BDSG. The TKG and the TMG have been amended and remain effective, but no longer contain data protection regulations. Whether this new legislation will actually put an end to the previous discussions remains to be seen.

Cookie compliance

The legal requirements with regard to the use of cookies were long unclear in Germany. It was disputed whether there was any consent requirement for cookies at all, as the respective provisions of the ePrivacy Directive had never been transposed into German law (which was also the opinion of the German data protection authorities at that time). Cookie consent was then required as of 28 May 2020, when the German Federal Court of Justice (*Bundesgerichtshof –* "**BGH**") ruled that Section 15 (3) TMG (which technically only provides for an opt-out requirement regarding the use of cookies) was to be construed as a requirement for cookie consent in the meaning of the ePrivacy Directive.

With Section 25 TTDSG, Germany finally transposed Article 5 (3) of the ePrivacy Directice into national law in December 2021, making cookie consent a legal obligation while explicitly including the definition of consent in terms of the GDPR.

In accordance with the ePrivacy Directive, under German law consent is not required where the sole purpose of cookies (or to be more precise, of the storage of information or access to information already stored in the users terminal equipment) is carrying out the transmission of a communication over a public telecommunications network or providing a telemedia service explicitly requested by a user (Section 25 (2) TTDSG).

In addition to that, the German data protection authorities have long been of the opinion that the processing of personal data enabled by the cookies used for analysis and tracking tools regularly requires consent, in particular if the tools allow third parties to collect data from website users as (joint) controllers. It remains to be seen whether this position will be upheld by the BGH or another superior German court.

Traffic data

Lawful processing of traffic data is governed by Section 9 et. seqq. TTDSG and may only take place to the extent it is necessary for the purposes constituted therein or if

other legal provisions require a processing. Those who provide or participate in the provision of telecommunication services have to take the technical precautions and actions necessary to protect personal data in accordance with Section 165 TKG; in this context the state of the art must be observed. In addition, the service providers are required to protect the secrecy of telecommunications, which extends to both the content of telecommunications and its detailed circumstances, in particular the fact whether someone is or was involved in a telecommunications process.

Providers of telecommunication services in terms of Section 3 (2) sentence 1 TTDSG may process traffic data for the establishment and maintaining of a telecommunications connection, remuneration inquiry and billing, fraud prevention as well as detection and remedy of disruptions regarding telecommunications systems and tracing of malicious or nuisance calls. Processing of traffic data for marketing purposes, need-based design of telecommunication services and provision of value-added services requires consent in accordance with GDPR.

Generally, traffic data shall be deleted by the service provider without undue delay after termination of each telecommunications connection or as soon as the data are no longer necessary in relation to the purpose for which they are otherwise being processed. However, data may and must be stored in case statutory retention periods under the TTDSG, TKG or other law apply.

If there is a particular and significant risk of a security incident, providers of publicly available telecommunication services shall notify the users about any possible protective or remedial measures that can be taken by users and, where appropriate, about the threat itself (Section 168 (6) TKG), in addition to their general notification obligations with respect to security incidents towards the German Federal Network Agency (*Bundesnetzagentur* – "**BNetzA**") and the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – "**BSI**").

Location data

Publicly available telecommunication services may only process location data for the purpose of providing value-added services in case the data are rendered anonymous or processing is based on consent in terms of the GDPR (Section 13 (1) TTDSG).

Consent can be withdrawn at any time and where consent was given to the processing of location data, it must be possible, by simple means and free of charge, to

temporarily prohibit the processing of such data for each connection to the network or for each transmission of a message.

The processing of location data in other contexts than telecommunication services (like for example GPS tracking) is subject to the GDPR.

KEY CONTACTS

Goldfarb Seligman & Co., Law Offices
www.goldfarb.com

Sharon Aloni
Partner
Goldfarb Seligman & Co., Law Offices
T +972 (3) 608 9834
sharon.aloni@goldfarb.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.

KEY CONTACTS

Verena Grentzenberg
Partner
T +49 40 188 88 203
verena.grentzenberg@dlapiper.c

Dr. Jan Geert Meents
Partner
T +49 89 23 23 72 130
jan.meents@dlapiper.com

Jan Pohle
Partner
T +49 221 277 277 391
jan.pohle@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.