# Comparing privacy laws:
# GDPR v. PPL

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

## About the authors

**OneTrust DataGuidance™** provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

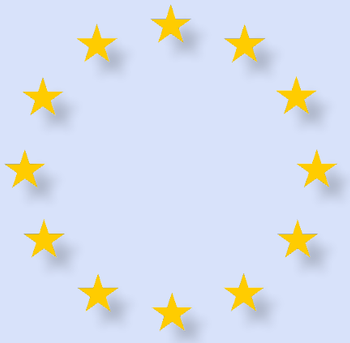
The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare PPL across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Image production credits:
Cover/p.5/p.51: 221A / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com



# Table of contents



# Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect on 25 May 2018, and governs the protection of personal data in EU and EEA Member States. The Protection of Privacy Law, 5741-1981 ('the PPL') is the main legislation governing the protection of privacy in Israel. The PPL covers the right to privacy afforded to all persons in Israel and the information security requirements for those managing databases containing personal information and sensitive information. The Privacy Protection Authority ('PPA') PPLs as the supervisory authority and the head of the PPA also serves as the Registrar of Databases. Article 36 of the PPL allows the Minister of Justice to make regulations as to any matter relating to its implementation. For instance, in 2017, the PPA issued the Protection of Privacy (Data Security) Regulations, 5777-2017 ('the Data Security Regulations') which establish more specific rules of conduct for database owners, possessors, and managers regarding the security of databases.

The GDPR and the PPL contain many similarities, and, in particular, have comparable provisions regarding specific roles and responsibilities for those handling personal data. A crucial fPPLor for organisations in Israel, however, is that privacy-related requirements revolve around the fPPL that organisations must register their databases in the Register of Databases. They must also ensure that, among other things, all uses of the information contained in the registered database comply with the purposes for which the database was established.

In 2020, the Ministry of Justice launched two public consultations which aimed to amend the PPL. In July 2020, the Ministry memorandum proposed the reduction of scope of the obligation to register a database and the amendment of key definitions. In November 2020, the Ministry of Justice launched a public consultation (only available in Hebrew here) on the PPL which requested comments on whether amendment to the law is required in order to bring it in line with current international standards such as the GDPR. The Ministry spotlighted specific focus areas, which included suggesting the establishment of additional legal bases for information processing, expanding data subject rights, introducing additional accountability requirements, strengthening the PPA's enforcement powers, removing the requirement for registration of a database, and adding requirements for specific groups.

Following the conclusion of the consultations, the Privacy Protection Bill (Amendment No. 14), 5722-2022, (only available in Hebrew here) ('Amendment No.14') is currently being discussed in the Israeli Parliament ('Knesset'), and would significantly amend the PPL. In particular, Amendment No.14 would introduce requirements for certain companies to appoint a data protection officer ('DPO'), as well as empower the PPA to impose enhanced penalties of NIS 3,200,000 (approx. €889,000) for certain offences.

Furthermore, the PPA has provided guidance on the requirements of a DPO in line with Amendment No.14 (only available in Hebrew here).

In addition to Amendment No.14, a private draft bill for Privacy Protection Law (Amendment - Reinforcement of the Right to Privacy and its Protection), 2022 ('the Bill') has also been submitted to the Knesset. Although there is some duplication between Amendment No.14 and the Bill, the latter proposes a more comprehensive framework aimed at aligning the PPL with modern data protection laws, such as the GDPR, and includes, inter alia, a definition of the roles of the PPA, additional data subject rights, such as the right to be forgotten, and clarification of the extraterritorial applicability of the PPL.

This overview organises provisions from the GDPR and the current version of the PPL into key topics and sets them alongside each other to enable analysis and comparison. Each section begins with a detailing of principal information and a general introduction, as well as a consistency rating.

## Structure and overview of the Guide

This Guide provides a comparison of the two legislative frameworks on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant provisions from the two legislative legal frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the PPL.

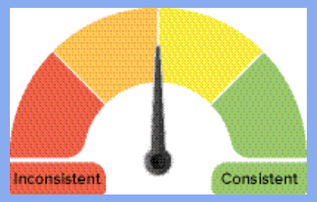
### Key for giving the consistency rate

**Consistent:** The GDPR and the PPL bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

**Fairly consistent:** The GDPR and the PPL bear a high degree of similarity in the rationale, core, and the scope of the provision considered, however, the details governing its application differ.

**Fairly inconsistent:** The GDPR and the PPL bear several differences with regard to the scope and application of the provision considered, however, its rationale and core presents some similarities.

**Inconsistent:** The GDPR and the PPL bear a high degree of difference with regard to the rationale, core, scope, and application of the provision considered.




## Usage of the Guide

This Guide is general and informational in nature, and is not intended to provide, and should not be relied on as a source of, legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be PPLed upon without specific legal advice based on particular circumstances.



# 1. Scope


## 1.1. Personal scope

There are various similarities in personal scope between the GDPR and the PPL in relation to data controllers, data processors, and public bodies. A major difference, however, is that the PPL provides for data subject rights after death and any related complaints. Furthermore, the PPL applies to databases owned by corporate bodies and public bodies, with specific requirements for each.

| GDPR | PPL |
|---|---|

### Data controller

Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Section 8(c): A database owner is obligated to register his database in the Registry, and he shall register the database if one of the following applies: (1) the database contains information on more than 10,000 persons; (2) the database contains sensitive information; (3) the database includes information on persons, and the information was not delivered to this database by them, on their behalf or with their consent to this database; (4) the database belongs to a public body as defined in Section 23; (5) the database is used for direct-mailing services as referred to in Section 17C.

### Data processor

Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Section 7: 'Manager of database' means an active manager of a body that owns or possesses a database or a person whom the aforesaid manager authorized for this purpose.
Section 3: 'Possessor, for the purpose of a database' means a person who has a database in his possession permanently and is permitted to use it.

### Data subject

Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fPPLors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

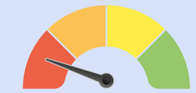
Section 3: A 'person' for the purposes of Sections 2, 7, 13, 14, 17B, 17C, 17F, 17G, 23A, 23B and 25, does not include a body corporate.
[Note: Section 1 of the Privacy Protection (Data Security) Regulations, 5777 – 2017 ('Data Security Regulations') defines 'data subject' as the person on which the database contains information.]

| GDPR | PPL |
|---|---|
| **Public bodies** | |
| Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body. | Section 23: 'public body' means (1) a Government Department and any other State institution, a local authority and any other body carrying out public functions under any law; (2) a body designated by the Minister of Justice, by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, provided that the order shall prescribe the categories of information and data items which the body may impart and receive. |
| **Nationality of data subject** | |
| Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data. | The PPL does not explicitly refer to the nationality of persons, however the right to privacy applies in the State of Israel. |
| **Place of residence** | |
| See Recital 14, above. | The PPL does not explicitly refer to application to the place of resident, however the right to privacy applies in the State of Israel and Section 14 of the PPL notes that, regarding the exercise of the right to inspection, if the database owner is not a resident, the database possessor should amend or delete the relevant information. |
| **Deceased individuals** | |
| Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons. | Section 25: (a) Where a person whose privacy has been infringed dies within six months after the infringement without having filed an action or complaint in respect thereof, his spouse, child or parent or, if he leaves no spouse, child or parent, his brother or sister may file an action or complaint in respect of that infringement within six months after his death. (b) Where a person who has filed an action or complaint in respect of an infringement of privacy dies before the termination of the proceeding, his spouse, child or parent or, if he leaves no spouse, child or parent, his brother or sister may, within six months after his death, notify the court that he or she wishes to proceed with the action or complaint, and upon so notifying, he or she shall take the place of the plaintiff or complainant. Section 17F(f): The rights under this section of a deceased person recorded in a database are given also to his spouse, child, parent or sibling. [Note: Section 17F of the PPL regulates the right to erasure in relation to direct marketing.] |





## 1.2. Territorial scope



**Inconsistent**

Where the GDPR regulates entities established within the territory of the EU, the PPL does not particularly specify its territorial scope beyond that applications for registration must state the addresses in Israel of the database owner, possessor, and manager. Therefore, territorial scope is limited to Israel. Furthermore, unlike the GDPR, the PPL does not explicitly refer to goods and services from abroad and extraterritorial scope.

| GDPR | PPL |
|---|---|
| **Establishment in jurisdiction** | |
| Article 3: This Regulation applies to the processing of personal data in the context of the PPLivities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Recital 22: Establishment implies the effective and real exercise of PPLivity through stable arrangements. | Section 8(a): No person shall manage or possess a database that requires registration pursuant to this Section, unless one of the following has occurred: (1) the database has been registered in the Register; (2) an application has been made to register the database and the provisions of Section 10(B1) have been met; (3) the database requires registration pursuant to subsection (e) and the Registrar's order permitted management and possession of the database until the time of its registration. |
| **Extraterritorial** | |
| See Article 3, above. | The PPL does not explicitly refer to extraterritorial application. |
| **Goods & servicies from abroad** | |
| Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing PPLivities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. | The PPL does not explicitly refer to its application regarding goods and services from abroad. |
| **Monitoring from abroad** | |
| Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union. | The PPL does not explicitly refer to its application regarding monitoring from abroad. |

# 1.3. Material scope

**Fairly inconsistent**

Both the GDPR and the PPL regulate the processing or use of personal data or information respectively, and specify further requirements for information that is considered sensitive. The PPL does not refer to anonymised or pseudonymised data. However, it does establish what constitutes infringements of privacy in its opening provisions as a basis against which the requirements that follow are set out.

| GDPR | PPL |
|---|---|

## Personal data/ personal information

Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fPPLors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Section 7: 'Information' means data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.
Section 1: No person shall infringe the privacy of another without his consent.
Section 2: Infringement of privacy is any of the following:
(1) spying on or trailing a person in a manner likely to harass him, or any other harassment;
(2) listening-in prohibited under any Law;
(3) photographing a person while he is in the private domain;
(4) publishing a person's photograph under such circumstances that the publication is likely to humiliate him or bring him into contempt;
(5) copying or using, without permission from the addressee or writer, the contents of a letter or any other writing not intended for publication, unless the writing is of historical value or 15 years have passed since the time of writing. In this section 'writing' - including electronic message as defined in Electronic Signature Law, 5761 – 2001 (only available in Hebrew here);
(6) using a person's name, appellation, picture or voice for profit;
(7) infringing a duty of secrecy laid down by law in respect of a person's private affairs;
(8) infringing a duty of secrecy laid down by express or implicit agreement in respect of a person's private affairs;
(9) using, or passing on to another, information on a person's private affairs otherwise than for the purpose for which it was given;
(10) publishing or delivering anything obtained by way of an infringement of privacy under paragraphs (1) to (7) or (9);
(11) publishing any matter relating to a person's intimate life, including his sexual history, state of health or conduct in the private domain.



| GDPR | PPL |
|---|---|

## Data processing

Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Section 3: 'Use' includes disclosure, transfer and delivery of information.

## Special categories of data

Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Section 7: 'Sensitive information' means - (1) data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person; (2) information that the Minister of Justice determined by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, is sensitive information.

## Anonymised data

Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The PPL does not specifically refer to anonymised data.

## Pseudonymised data

Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

The PPL does not specifically refer to pseudonymised data.

| GDPR | PPL |
|---|---|

## Automated processing

Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

According to the definition of 'database' under Section 7, the PPL applies to the collection of data intended for computer processing.

## General exemptions

Article 2(2): This Regulation does not apply to the processing of personal data:
(a) in the course of an PPLivity which falls outside the scope of Union law;
(b) by the Member States when carrying out PPLivities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; or
(c) by a natural person in the course of a purely personal or household PPLivity.

Section 7 provides the following exceptions from the definition for 'database', and therefore the provisions relating to databases: (1) a collection for personal use that is not for business purposes; or (2) a collection that includes only the name, address and method of communication, which in itself does not produce a characterization which infringes the privacy of the persons whose names are included therein, provided that the owner of the collection or the body corporate under his control does not have another collection. Furthermore, Chapter Three covers defenses which can be used in any criminal or civil proceedings for the infringement of privacy.



# 2. Key definitions


## 2.1. Personal data

Although both the GDPR and the PPL apply to personal data and information relating to persons, the definition in the PPL is in the form of a more generalised discussion of categories rather than specific examples. In this manner, the PPL extends its definition to, for example, personality and opinions and beliefs. However, the PPL is specific in its definition of photography as information.

| GDPR | PPL |
|---|---|

## Personal data/ personal information

Article 4(1): 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more fPPLors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Section 7: 'Information' means data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person.

## Special categories of data

Article 9(1): Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Section 7: 'Sensitive information' means - (1) data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person; (2) information that the Minister of Justice determined by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, is sensitive information.

## Online identifiers

Recital 30: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

The PPL does not explicitly refer to online identifiers.

| GDPR | PPL |
|---|---|
| **Other (Photography)** | |
| Recital 51: The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.<br>Article 4(14): 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data. | Section 3 defines 'photography' as including filming. Section 2 clarifies that publishing a person's photograph under such circumstances that the publication is likely to humiliate him or bring him contempt or photographing a person while they are in the private domain both constitute an infringement of privacy.<br>Section 1 of the Data Security Regulations defines 'biometric data' as information used to identify a person which is a unique physiological human characteristic that can be measures by a computer. |

## 2.2. Pseudonymisation


The GDPR defines and discusses anonymised and pseudonymised data, while the PPL does not directly address these topics.

| GDPR | PPL |
|---|---|
| **Anonymisation** | |
| Recital 26: 'anonymous information' is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. | The PPL does not explicitly refer to the anonymisation of data. |
| **Pseudonymisation** | |
| Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. | The PPL does not explicitly refer to the pseudonymisation of data. |

# 2.3. Controllers and processors

**Fairly consistent**

The concepts of data protection officers ('DPO'), data controllers, and processors under the GDPR are comparable to the concepts of security supervisors, database owners, and database managers or possessors in the PPL. Furthermore, both the GDPR and the PPL provide for the establishment of agreements between these entities. However, the PPL does not contain a legal requirement for Data Protection Impact Assessments ('DPIA').

| GDPR | PPL |
|---|---|

## Data controller

Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Section 8(c): A database owner is obligated to register his database in the Registry, and he shall register the database if one of the following applies: (1) the database contains information on more than 10,000 persons; (2) the database contains sensitive information; (3) the database includes information on persons, and the information was not delivered to this database by them, on their behalf or with their consent to this database; (4) the database belongs to a public body as defined in Section 23; (5) the database is used for direct-mailing services as referred to in Section 17C.

## Data processor

Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Section 7: 'Manager of database' means an active manager of a body that owns or possesses a database or a person whom the aforesaid manager authorized for this purpose. Section 3: 'Possessor, for the purpose of a database' means a person who has a database in his possession permanently and is permitted to use it.

## Controller and processor contracts

Article 28(3): Processing by a processor shall be governed by a contrPPL or other legal PPL under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [Article 28 goes on to stipulate necessary information to be included in such a contrPPL.]

Section 17A: (a) A person who possesses databases of different owners shall ensure that access to each database is provided only to persons who are expressly authorized to do so by written agreement between the person and the owner of the said database. (b) A person who possesses at least five databases that require registration under Section 8 shall deliver annually to the Registrar a list of the databases in his possession, indicating the names of the owners of the databases, verified by affidavit that, in respect of each of the databases, the persons entitled to access to the database were determined by agreement between the person and the owner, and the name of the security supervisor, as referred to in Section 17B.



| GDPR | PPL |
|---|---|

## Data Protection Impact Assessment ('DPIA')

DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information).

There is no legal requirement to conduct a DPIA or privacy impact assessment ('PIA').

## Data Protection Officer ('DPO')

DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. for further information).

Section 17B: A person with the appropriate qualifications to be in charge of the information security (hereinafter – security supervisor): (1) a possessor of five databases that require registration under Section 8; (2) a public body as defined in Section 23; (3) a bank, an insurance company, a company involved in rating or evaluating credit. (b) Without derogating from the provisions of Section 17, the security supervisor shall be responsible for the information security in the databases kept in the possession of the bodies referred to in subsection (a) (c) A person who has been convicted of an offense involving moral turpitude or an offense of the provisions of the PPL shall not be appointed as security supervisor.

## 2.4. Children


The PPL does not distinguish between the definition of 'persons' and children. Furthermore, the PPL does not establish an age threshold or specific requirements for children beyond their role in relation to the rights of deceased family members (see 'deceased individuals' provisions in section 2.1. above).

| GDPR | PPL |
|---|---|

### Children's definition

The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

The PPL does not specifically define or provide an age threshold for 'children'.

### Consent for processing children's data

Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

The PPL does not distinguish between the consent of a child and a 'person'.

### Privacy notice (children)

Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

The PPL does not explicitly refer to addressing children within a privacy notice.



## 2.5. Research


The GDPR provides definitions and exceptions for the processing of personal data for the purposes of historical or statistical research purposes. However, the PPL does not include provisions for research, beyond a brief mention of processing information from writings of 'historical value.'

| GDPR | PPL |
|---|---|

### Scientific/ historical research definition

Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research.
Recital 160: Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.

The PPL does not explicitly refer to scientific or historical research. However, Section 2(5) of the PPL indicates that, if the writing (or electronic message) is of historical value or 15 years have passed since the time of writing, then the copying or using, without permission from the addressee or writer, the contents of a letter or any other writing not intended for publication, does not constitute an infringement of privacy.

### Compatibility with original purpose of collection

Article 5(1)(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').

The PPL does not explicitly refer to research and compatibility with the original purpose of collection.

### Appropriate safeguards

Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner.

The PPL does not explicitly refer to appropriate safeguards required for processing for archiving purposes.

| GDPR | PPL |
|---|---|

## Data subject rights (research)

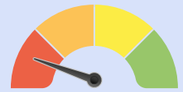
Under Article 17(3), the right to erasure may not apply in cases of scientific or historical research. Article 21(6), however, provides that data subjects may exercise the right to object to data processing for scientific or historical research purposes. In addition, Article 89 provides that Member States may derogate from the GDPR in regard to data subject rights and data processing for research purposes.

The PPL does not explicitly refer to data subject rights relating to research.





# 3. Legal basis



Inconsisntent

The PPL does not explicitly refer to legal bases for processing personal information. Instead, it clarifies that no person shall infringe the privacy of another without his consent and offers some defenses that can be used in legal proceedings regarding an infringement of privacy after the fact which cover, among other things, intention, legal obligations and legitimate personal interests.

| GDPR | PPL |
|---|---|

## Legal grounds

Article 6(1): Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contrPPL to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contrPPL;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The PPL does not explicitly refer to legal grounds for processing. However, Section 1 of the PPL states that 'no person shall infringe the privacy of another without his consent.'

Chapter Three lists what constitutes a 'good defence' in any criminal or civil proceeding for the infringement of privacy. Section 18 provides that a 'good defence' might be that:

(1) the infringement was committed by way of a publication protected under Section 13 of the Defamation Law;

(2) the defendant or accused committed the infringement in good faith and in any of the following circumstances: (a) he did not know and need not have known that an infringement of privacy might occur; (b) the infringement was committed in circumstances in which the infringer was under a legal, moral, social or professional obligation to commit it; (c) the infringement was committed in defence of a legitimate personal interest of the infringer; (d) the infringement was committed in the lawful pursuit of the infringer's occupation and in the ordinary course of his work, so long as it was not committed by way of publication; (e) the infringement was committed by way of taking a photograph, or of publishing a photograph taken, in the public domain, and the injured party appears in it accidentally; (f) the infringement was committed by way of a publication protected under paragraphs (4) to (11) of Section 15 of the Defamation (Prohibition) Law, 5725 – 1965 (only available in Hebrew here) ('the Defamation Law') ; (3) The infringement involved a public interest justifying it in the circumstances of the case, provided that, if the infringement was committed by way of publication, the publication was not untruthful.

| GDPR | PPL |
|---|---|

## Sensitive data (legal basis)

There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.

Section 2(11) of the PPL states that publishing any matter relating to a person's intimate life, including his sexual history, state of health or conduct in the private domain constitutes an infringement of privacy.

## Conditions for consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Article 4: (11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative PPLion, signifies agreement to the processing of personal data relating to him or her.

Section 3 of the PPL defines 'consent' as informed, express, or implied consent.

## Journalism/artistic purposes

Article 85(1): Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.

The PPL does not explicitly refer to journalism or artistic purposes.



# 4. Controller and processor obligations

## 4.1. Data transfers

Fairly consistent

The PPL itself does not specify mechanisms to enable data transfers. However, it does allow the Minister of Justice to clarify requirements for such transfers in additional regulations. In response to this, the Data Security Regulations indicate what information on data transfers is required in the database definitions document and the use of encryption methods.

| GDPR | PPL |
|---|---|

## Adequate protection

Article 45(1): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

The PPL does not include any information on adequate protection of transfers of personal data to third countries. However, in 2011, Israel was recognised by the European Commission as providing an adequate level of protection for personal data.

## Other mechanisms for data transfers

Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
(2) The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
(a) a legally binding and enforceable instrument between public authorities or bodies;
(b) binding corporate rules in accordance with Article 47;
(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);

Section 9 of the PPL states that an application for registration of a database to the Registrar must include details on the transfer of information abroad. Furthermore, Section 36 stipulates that the Minister of Justice may make regulations regarding the conditions of transmitting information to or from databases outside of Israel.
Section 2 of the Data Security Regulations further details: the database definitions document must include details regarding the transfer of the database or substantial parts thereof outside the State borders or the use of the data outside the State borders, the purpose of transfer, country of destination, and the identity of the transferee. [...] The database controller will update the database definitions document whenever a significant change has been made.
Section 14 of the Data Security Regulations specify that the transfer of information from the database through a public network or the Internet will be conducted by commonly used encryption methods.

| GDPR | PPL |
|---|---|

## Other mechanisms for data transfers (cont'd)

(c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
(d) standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2);
(e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
(f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
(3) Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by:
(a) contrPPLual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
(b) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

## Data localisation

Not applicable.

The PPL does not explicitly refer to data localisation requirements.





# 4.2. Data processing records


Both the PPL and the GDPR contain general documentation requirements, although the GDPR provides more detail on these records. The PPL does, however, establish registration obligations and discusses these in depth. There is also further information on record keeping in the Data Security Regulations.

| GDPR | PPL |
|---|---|

## Data controller obligation

Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing PPLivities under its responsibility. That record shall contain all of the following information:

(a) the name and contPPL details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data; and

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

The PPL does not specify the requirement for a record of processing activities. However, Section 2 of the Data Security Regulations provides: A database controller will specify in the database definitions document (the 'database definitions document') at least the following matters: (1) A general description of the data collection and usage activities; Database definitions document is binding and the reader is advised to consult the authoritative Hebrew text.
(2) A description of the purposes for which the data is used;
(3) The types of data contained in the database, in accordance with the list of data types in Item 1(3) of the First Schedule;
(4) Details regarding the transfer of the database or substantial parts thereof outside the State borders or the use of the data outside the State borders, the purpose of transfer, country of destination, manner of transfer and the identity of the transferee;
(5) Data processing activities by a processor;
(6) The main risks concerning a breach of information security and the manner in which they are dealt with;
(7) The name of the database manager, the database processor and the data security officer, if appointed. (b) The database controller will update the database definitions document whenever a significant change has been made to the matters detailed in Sub-Regulation (a) and will annually assess, by 31 December of each year, the need for such an update due to technological changes within the organization or security incidents as per Regulation 11. (c) The database controller will review annually whether the data stored in the database exceeds what is required for the database purposes. Furthermore, there are general requirements for documentation in the PPL, such as Section 17E: A person shall not manage or possess a database used for direct mailing services, unless he has a record indicating the source from which he received every collection of data used for the database, and the date it was received, and to whom each said collection of data was delivered.

| GDPR | PPL |
|---|---|

## Data controller obligation (cont'd)

| | |
|---|---|
| | Section 10 of the PPL: In carrying out his functions, an inspector may demand every relevant person to deliver to him information and documents relating to a database. Section 31A of the PPL: a person who fails to provide the Registrar documents is subject to imprisonment for one year. |

## Data processor obligation

| | |
|---|---|
| Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing PPLivities carried out on behalf of a controller, containing: (a) the name and contPPL details of the processor or processors and of each controller on behalf of which the processor is PPLing, and, where applicable, of the controller's or the processor's representative, and the data protection officer; (b) the categories of processing carried out on behalf of each controller; (c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). | See requirements from the Data Security Regulations and the PPL above. |

## Records format

| | |
|---|---|
| Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form. | The PPL does not explicitly discuss the format of a record of processing activities. |

## Required to make available

| | |
|---|---|
| Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request. | The PPL does not explicitly refer to records of processing activities. However, under Section 31A of the PPL: A person who fails to provide the Registrar documents is subject to imprisonment for one year. |



| GDPR | PPL |
|---|---|

## Exemptions

| | |
|---|---|
| Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10. | The PPL does not provide exemptions for database definitions documents. |

## General Data Processing Notification ('DPN')

| | |
|---|---|
| Not applicable. | The PPL does not explicitly refer to general data processing notifications. However, under Section 8 of the PPL: A database owner is obligated to register his database in the Registry, and he shall register the database if one of the following applies: (1) the database contains information on more than 10,000 persons; (2) the database contains sensitive information; (3) the database includes information on persons, and the information was not delivered to this database by them, on their behalf or with their consent to this database; (4) the database belongs to a public body as defined in Section 23; (5) the database is used for direct-mailing services as referred to in Section 17C. |

# 4.3. Data protection impact assessment


The GDPR sets out requirements for conducting a Data Protection Impact Assessment ('DPIA'), where the PPL does not. The Data Security Regulations, however, require high-security databases to conduct risk assessments. However, the PPA has issued a non-binding framework for PIAs, which recommends carrying out a PIA under certain circumstances and includes a template for the same (only available in Hebrew here).

| GDPR | PPL |
|---|---|

## When is a DPIA required

Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impPPL of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
[...] (3) A data protection impPPL assessment referred to in paragraph 1 shall in particular be required in the case of:
(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
(c) a systematic monitoring of a publicly accessible area on a large scale.

The PPL does not explicitly refer to DPIAs.
Section 5(c) of the Data Security Regulations: In a database subject to high security level, the database controller is responsible to conduct a data security risk assessment (the 'risk assessment'); the database controller will discuss the findings of the risk assessment provided to him, consider the need to update the database definitions document or the data security procedure as a result, and act to amend the shortcomings found in the course of the assessment, if any; such risk assessment will take place at least once every 18 months.

## DPIA content requirements

Article 35(7): The assessment shall contain at least:
(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance

The PPL does not explicitly refer to DPIAs.



| GDPR | PPL |
|---|---|

## DPIA content requirements

with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

## Consultation with authority

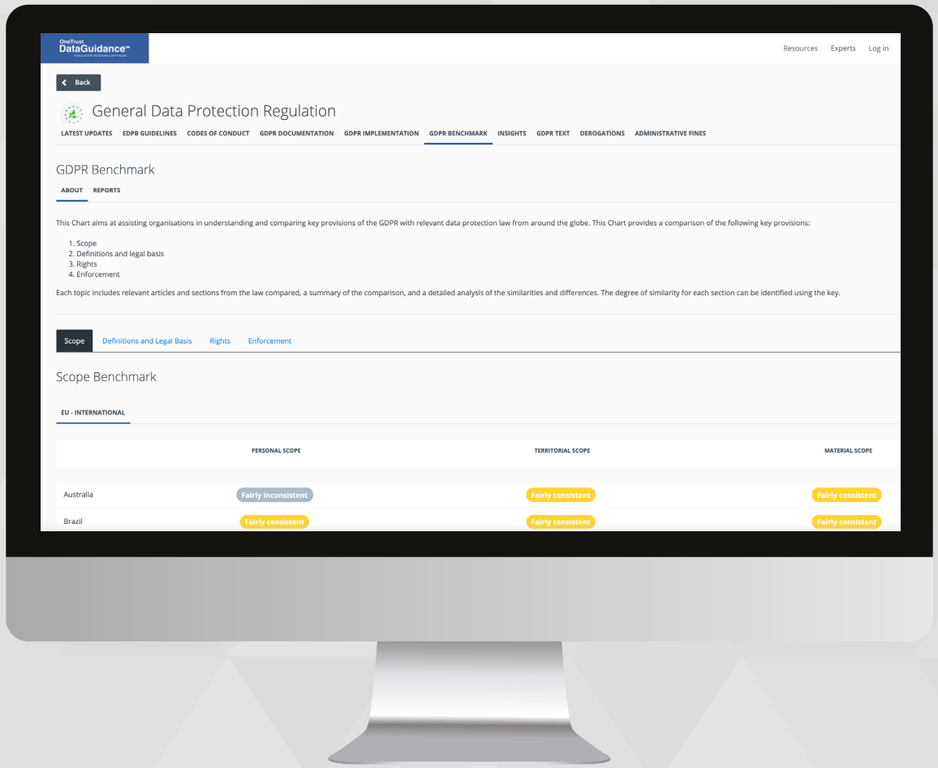
Article 36(1): The controller shall consult the supervisory authority prior to processing where a data protection impPPL assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. [Article 36 goes on to detail requirements related to such prior consultation].

The PPL does not explicitly refer to DPIAs.

# Global Regulatory Research Software

## 40 In-House Legal Researchers, 500 Lawyers Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk, and achieve global compliance




## Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan | China
and 20+ other global laws & frameworks

### Understand and compare key provisions of the GDPR with relevant data protection laws from around the globe

The GDPR Benchmarking tool provides comparison of the various pieces of legislation on the following key provisions

- Scope
- Rights
- Definitions and legal basis
- Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

OneTrust
**DataGuidance™**
REGULATORY RESEARCH SOFTWARE

Start your free trial at
**www.dataguidance.com**

# 4.4. Data protection officer appointment


The PPL provides for a similar position as the GDPR's DPO in the form of a security supervisor (sometimes referred to as a data security officer). However, the PPL does not include as extensive obligations regarding qualifications, everyday tasks, or group appointments.

| GDPR | PPL |
|---|---|

## DPO tasks

Article 39(1): The data protection officer shall have at least the following tasks:
(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
(c) to provide advice where requested as regards the data protection impPPL assessment and monitor its performance pursuant to Article 35;
(d) to cooperate with the supervisory authority; and
(e) to PPL as the contPPL point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

Section 17B: Without derogating from the provisions of Section 17, the security supervisor shall be responsible for the information security in the databases kept in the possession of the bodies referred to in subsection (a).

Furthermore, Section 3 of the Data Security Regulations indicates that, where a security supervisor is appointed, the security supervisor must prepare a data security procedure and have it approved by the database manager, prepare a plan for regular monitoring in regard to compliance with the Data Security Regulations, implement the plan and notify the database controller and the database manager of any findings.

Section 3(4) of the Data Security Regulations highlights that the security supervisor must not perform any additional role which may put them at risk of conflict of interest.

## When is a DPO required

Article 37(1): The controller and the processor shall designate a data protection officer in any case where:
(a) the processing is carried out by a public authority or body, except for courts PPLing in their judicial capacity;
(b) the core PPLivities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
(c) the core PPLivities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Section 17B of the PPL provides that the following bodies should appoint a security supervisor:
(1) a possessor of five databases that require registration under Section 8;
(2) a public body as defined in Section 23;
(3) a bank, an insurance company, a company involved in rating or evaluating credit.



| GDPR | PPL |
|---|---|

## Group appointments

Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

The PPL does not explicitly refer to group appointments.

## Notification of DPO

Article 37(7): The controller or the processor shall publish the contPPL details of the data protection officer and communicate them to the supervisory authority.

Section 17A(b): A person who possesses at least five databases that require registration under Section 8 shall deliver annually to the Registrar a list of the databases in his possession, indicating the names of the owners of the databases, verified by affidavit that, in respect of each of the databases, the persons entitled to access to the database were determined by agreement between the person and the owner, and the name of the security supervisor, as referred to in Section 17B.

## Qualifications

Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and prPPLices and the ability to fulfil the tasks referred to in Article 39.

According to Section 17B of the PPL, security supervisors must have the appropriate qualifications to be in charge of information security. Furthermore, Section 17B(c) provides: a person who has been convicted of an offense involving moral turpitude or an offense of the provisions of the PPL shall not be appointed as security supervisor.

# 4.5. Data security and data breaches


The PPL does not contain requirements regarding breaches and data security, whereas the GDPR includes extensive requirements. Instead, the Data Security Regulations cover data security and breach notification requirements to the PPA. The Data Security Regulations define a 'security incident' as a breach of integrity, unauthorised use thereof or deviation from authorisation. In Israel, database controllers are only initially required to notify the PPA, who may then decide to notify any further parties.

| GDPR | PPL |
|---|---|

## Security measures defined

Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(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;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The Data Security Regulations provide requirements for ensuring the security of databases. In particular, the Data Security Regulations outline appropriate measures regarding the writing of a binding data security procedure (Section 4), mapping of database systems and risk assessments (Section 5), physical protection and secure surroundings (Section 6), data security in manpower management (Section 7), access permissions management (Section 8), identification and authentication (Section 9), monitoring and documenting access (Section 10), portable devices (Section 12), secure and updated management of database systems (Section 13), network security (Section 14), outsourcing (Section 15), periodical audits (Section 16), retaining security data (Section 17), and data backup and restoration (Section 18). Under Section 1 of the Data Security Regulations, a severe security incident is defined as: (1) In a database subject to high security level - an incident involving the use of data from the database without authorization or in excess of authorization, or damage to the data integrity; (2) In a database subject to medium security level - an incident involving the use of substantial part of the database without authorization or in excess of authorization, or damage to the data integrity with respect to a substantial part of the database.

## Data breach notification to authority

Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The PPL does not cover data breach notifications. Section 11(d) of the Data Security Regulations provides, in the case of a severe security incident: The database controller will immediately notify the Registrar and report to the Registrar on the measures he took following the incident.



| GDPR | PPL |
|---|---|

## Timeframe for breach notification

See Article 33(1) above.

The PPL does not cover data breach notifications or timeframes. In addition, see Section 11(d) of the Data Security Regulations above.

## Notifying data subjects of data breach

Article 34(1): When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The PPL does not cover data breach notifications. The Data Security Regulations do not require that a breach be notified to the data subject, except in case of a severe security incident where Section 11(d) provides: The Registrar may order a database controller, except a controller of the databases listed in Section 13(e) of the Law, and after consulting with the head of the National Cyber Defense Authority, to give a notice of the security incident to a data subject who may suffer damage as a result of the incident.

## Data processor notification of data breach

Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

The PPL does not cover data breach notifications. Section 19 of the Data Security Regulations: The obligations that apply in these Regulations to a database controller will also apply to a database manager, and with the exception of the obligations prescribed in Regulations 2 and 15(a), they will also apply to the database processor, with the necessary changes as relevant.

## Exceptions

Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

The PPL does not cover data breach notifications. See Section 1 of the Data Security Regulations, above, on the definition of a severe security incident.

## 4.6. Accountability


Section 17 of the PPL covers the responsibility for information security, which is held by both the database owner and the database possessor/manager. Likewise the PPL and the GDPR both define different roles and responsibilities for the database owner/data controller as well as the database manager or possessor/data processor.

| GDPR | PPL |
|---|---|

### Principle of accountability

Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). [Paragraph 1 details principles of: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.]

Section 17: A database owner, possessor or manager, are each responsible information security for the information security in the database.

### Liability of data controllers and data processors

Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has PPLed outside or contrary to lawful instructions of the controller.

Section 17A: (a) A person who possesses databases of different owners shall ensure that access to each database is provided only to persons who are expressly authorized to do so by written agreement between the person and the owner of the said database. (b) A person who possesses at least five databases that require registration under Section 8 shall deliver annually to the Registrar a list of the databases in his possession, indicating the names of the owners of the databases, verified by affidavit that, in respect of each of the databases, the persons entitled to access to the database were determined by agreement between the person and the owner, and the name of the security supervisor, as referred to in Section 17B.





# 5. Rights


## 5.1. Right to erasure

Where the GDPR includes different categories of data subject rights, such as the right to erasure, the PPL focuses on persons and their right to inspection and amendment of information contained within a database.

| GDPR | PPL |
|---|---|

### Grounds for erasure

Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Section 14: (a) A person who, on inspecting any information about himself finds that it is not correct, not complete, not clear or not up to date may request the owner of the database or, if such owner is a non-resident, the possessor thereof to amend or delete the information.
(b) Where the owner of a database agrees to a request under subsection (a), he shall make the necessary changes in the information and shall notify them to every person who received the information from him within a period prescribed by regulations.
(c) Where the owner of a database refuses to comply with a request under subsection (a), he shall give notice to such effect, in the form and manner prescribed by regulations, to the person who made the request.
(d) The possessor is obligated to correct the information, if the owner of the database agreed to the requested correction or the court ordered that the correction be made.

### Inform data subject of right

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The PPL does not specifically address communication to the data subject of their rights.

| GDPR | PPL |
|---|---|

## Inform data subject of right

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

## Fees

Article 12(5): Information provided under Articles 13 and 14 and any communication and any PPLions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive charPPLer, the controller may either:
(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the PPLion requested; or
(b) refuse to PPL on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive charPPLer of the request.

Section 13(c2): The mode and conditions of, and the payment for, the exercise of the right of inspection of information shall be prescribed by regulations.

## Response timeframe

Article 12(3): The controller shall provide information on PPLion taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

Section 14(b): Where the owner of a database agrees to a request under subsection (a), he shall make the necessary changes in the information and shall notify them to every person who received the information from him within a period prescribed by regulations.



| GDPR | PPL |
|---|---|

## Format of response

Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

Section 14(c): Where the owner of a database refuses to comply with a request under subsection (a), he shall give notice to such effect, in the form and manner prescribed by regulations, to the person who made the request.

## Publicly available data

Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

The PPL does not explicitly address publicly available data.

## Exceptions

Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
(e) for the establishment, exercise or defence of legal claims.
Article 12(5): Information provided under Articles 13 and 14 and any communication and any PPLions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive charPPLer, the controller may either:

According to Section 13(c): Database owners may refuse to deliver to the person making the request information relating to his physical or mental health if, in his opinion, it is liable to severely harm the physical or mental health of the person making the request or endanger his life; in such case, the owner of the database shall deliver the information to a physician or psychologist on behalf of the person making the request. (c1) The provisions of this section shall not require the delivery of information in violation of a privilege prescribed by law, unless the person making the request is the person who is the beneficiary of the privilege.

| GDPR | PPL |
|---|---|

**Exceptions (cont'd)**

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
(b) refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.





# 5.2. Right to be informed

**Fairly inconsistent**

Where the GDPR includes different categories of data subject rights, such as the right to be informed, the PPL focuses on persons and their right to inspection and amendment of information contained within a database.

| GDPR | PPL |
|---|---|

**Informed prior to/ at collection**

Article 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:
(a) the identity and the contPPL details of the controller and, where applicable, of the controller's representative;
(b) the contPPL details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, the fPPL that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.
(2) In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to

Section 11: A request to a person for information with a view to the keeping and use thereof in a database shall be accompanied by a notice indicating –
(1) whether that person is under a legal duty to deliver that information or whether its delivery depends on his volition and consent;
(2) the purpose for which the information is requested;
(3) to whom the information is to be delivered and the purposes of such delivery.

| GDPR | PPL |
|---|---|

## Informed prior to/ at collection (cont'd)

withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contrPPLual requirement, or a requirement necessary to enter into a contrPPL, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

## What information is to be provided

See Article 13(1) and (2) above

See Section 11 above.

## When data is from third party

In addition to the information required under Article 13, Article 14(2) replaces the requirement that data subjects are provided with information on the legitimate interests pursued by the controller or by a third party, with an obligation to inform data subjects of the categories of personal data. Furthermore, paragraph (e) of Article 13(2) is replaced with a requirement to inform data subjects of the source from which the personal data originate, and if applicable, whether it came from publicly accessible sources.

Section 17E: A person shall not manage or possess a database used for direct mailing services, unless he has a record indicating the source from which he received every collection of data used for the database, and the date it was received, and to whom each said collection of data was delivered.

## Intelligibility requirements

Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The PPL does not explicitly refer to intelligibility requirements.



| GDPR | PPL |
|---|---|

## Format

See Article 12(1) above.

The PPL does not explicitly refer to the format of a response to an information request by the data subject.

## Exceptions

The requirements of Article 13 do not apply where the data subject already has the information.
The requirements of Article 14 do not apply where:
(a) the data subject already has the information;
(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
(d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

The PPL does not explicitly refer to exceptions to the right to be informed.

# 5.3. Right to object

Fairly inconsistent

The PPL does not provide a general right to object in the same manner as the GDPR. It does, however, contain relevant provisions for objecting to processing for direct marketing.

| GDPR | PPL |
|---|---|

## Grounds for right to object/ opt out

Article 21(1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

The PPL does not explicitly refer to a right to object. In general, Section 1 states that no person shall infringe the privacy of another without his consent and Section 2 defines infringing privacy as including, among other things, using a person's name, appellation, picture or voice for profit, and using, or passing on to another, information on a person's private affairs otherwise than for the purpose for which it was given.

## Withdraw consent

Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

The PPL does not explicitly refer to the withdrawal of consent.

## Restrict processing

Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

The PPL does not explicitly provide for data subjects to obtain a restriction of processing.



| GDPR | PPL |
|---|---|

## Object to direct marketing

Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

Section 17F: (a) Every contact by direct mailing shall include in a clear an conspicuous manner – (1) mention that the contact is direct mailing, indicating the registration number of the database being used for direct-mailing services as stated in the Register of databases; (2) notice of the right of the recipient of the contact to be removed from the database as referred to in subsection (b); along with the address which he should contact for this purpose; (3) the name and address of the owner of the database containing the information based on which the contact was made, and the sources from which the owner of the database received this information. (b) Every person is entitled to demand, in writing, of the owner of the database used for direct mailing that the information relating to him be deleted from the database. (c) Every person is entitled to demand, in writing, of the owner of the database used for direct-mailing services or of the owner of the database containing the information based on which the contact was made, that the information relating to him not be delivered to a person, to a type of persons or to specific persons, for either a limited period of time or permanently. (d) Where a person informed the owner of the database of his demand as specified in subsections (b) or (c), the owner of the database shall act in accordance with the demand and notify the person, in writing, that he acted accordingly. (e) Where the owner of the database did not give notice as specified in subsection (d) within 30 days from the day of receipt of the demand, the person whom the information is about may apply to the Magistrate's Court in the manner prescribed by regulations, to order the owner of the database to act as specified. (f) The rights under this section of a deceased person recorded in a database are given also to his spouse, child, parent or sibling.

## Inform data subject of right

See Article 12(1) in section 5.1. above. In addition, Article 21(4) provides: At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

The PPL does not explicitly refer to communication to data subjects of their rights.

| GDPR | PPL |
|---|---|
| **Fees** | |
| See Article 12(5) in section 5.1. above. | The PPL does not explicitly refer to a right to object. |
| **Format of response** | |
| See Article 12(1) in section 5.1. above. | The PPL does not address format of responses in relation to the right to object. |
| **Exceptions** | |
| See Article 12(5) in section 5.1. above. | See Section 10(2) of the PPL above. |

**Fairly consistent**

## 5.4. Right of access

The right to inspection in the PPL is similar to the right of access in the GDPR. However, the processes for exercising the right to inspection provided for in the PPL are not defined in the PPL itself.

| GDPR | PPL |
|---|---|
| **Grounds for right of access** | |
| Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. | Section 13(a): Every person is entitled to inspect, either himself or through a representative authorized by him in writing or his guardian, any information about him kept in a database. |
| **Information to be accessed** | |
| Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:<br>(a) the purposes of the processing;<br>(b) the categories of personal data concerned;<br>(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;<br>(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;<br>(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;<br>(f) the right to lodge a complaint with a supervisory authority;<br>(g) where the personal data are not collected from the data subject, any available information as to their source; and<br>(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. | Section 13: (a) Every person is entitled to inspect, either himself or through a representative authorized by him in writing or his guardian, any information about him kept in a database.<br>(b) The owner of a database shall enable, at the request of a person referred to in subsection (a) (hereinafter – person making the request) inspection of the information, in the Hebrew, Arabic or English language.<br>Furthermore, under Section 13A, when persons request to inspect information which is not in the possession of the database owner: (1) The owner of a database who keeps it at the place of another person (in this section - the possessor) shall refer owner of the database the person making the request to the possessor, with his address, and order the possessor, in writing, to enable the person making the request the inspection;<br>(2) Where the person making the request applies to the possessor first, the possessor shall inform him if he possesses information about him, and also the name and address of the owner of the database. |

| GDPR | PPL |
|---|---|

## Inform data subject of right

| GDPR | PPL |
|---|---|
| See Article 12(1) in section 5.1. | The PPL does not explicitly address the communication of rights to data subjects. |

## Fees

| GDPR | PPL |
|---|---|
| See Article 12(5) in section 5.1. above. | Section 13(c2): The mode and conditions of, and the payment for, the exercise of the right of inspection of information shall be prescribed by regulations. |

## Verify data subject request

| GDPR | PPL |
|---|---|
| Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to rePPL to potential requests. | The PPL does not explicitly address identity verification in relation to data subject requests. However, Section 13(c1) does stipulate that: the provisions of this section shall not require the delivery of information in violation of a privilege prescribed by law, unless the person making the request is the person who is the beneficiary of the privilege.<br>Section 9 of the Data Security Regulations provides general requirements regarding authentication and identification. |

## Response timeframe

| GDPR | PPL |
|---|---|
| See Article 12(3) in section 5.1. above. | Section 13(c2): The mode and conditions of, and the payment for, the exercise of the right of inspection of information shall be prescribed by regulations. |

## Format of response

| GDPR | PPL |
|---|---|
| See Article 12(1) in section 5.1. above. | Section 13(c2): The mode and conditions of, and the payment for, the exercise of the right of inspection of information shall be prescribed by regulations. |



| GDPR | PPL |
|---|---|

## Exceptions

| GDPR | PPL |
|---|---|
| See Article 12(5) in section 5.1. above. | Section 13(c): The owner of a database may refuse to deliver to the person making the request information relating to his physical or mental health if, in his opinion, it is liable to severely harm the physical or mental health of the person making the request or endanger his life; in such case, the owner of the database shall deliver the information to a physician or psychologist on behalf of the person making the request. (c1) The provisions of this section shall not require the delivery of information in violation of a privilege prescribed by law, unless the person making the request is the person who is the beneficiary of the privilege.<br>Section 13(c3): The provisions of this section shall not apply – (1) to a database of a security authority within the meaning of section 19(c); (1A) to a database of the Prisons Service; (2) to a database of a tax authority within the meaning of the Tax Law Amendment (Exchange of Information between Tax Authorities) Law, 5727 – 1967; (3) where the security or foreign relations of the State or the provisions of any enactment require that information about any person not be disclosed to him; (4) to any database, in respect of which the Minister of Justice, in consultation with the Minister of Defense or the Minister of Foreign Affairs, as the case may be, and with the approval of the Foreign Affairs and Security Committee of the Knesset, has determined that it contains information as to which the security or foreign relations of the State requires or require that it not be disclosed (such information hereinafter referred to as 'secret information'), provided that a person wishing to inspect information about himself kept at any such database shall be entitled to inspect information other than secret information. (5) to a database about investigations and law enforcement of an authority empowered to investigate by law an offense, which the Minister of Justice determined by order, with the approval of the Constitution, Law and Justice Committee of the Knesset. (6) to a database established under Section 28 of the Prohibition on Money Laundering Law, 5760 –2000 (only available to download in Hebrew here). |

## 5.5. Right not to be subject to discrimination

Fairly consistent

Neither the GDPR nor the PPL define a right not to be subject to discrimination. However, it can be implied in general concepts, such as fairness and lawful processing in the GDPR and information integrity in the PPL.

| GDPR | PPL |
|---|---|

### Definition of right

The GDPR only implies this right and does not provide an explicit definition for it.

The PPL does not explicitly define a right not to be subject to discrimination.

### Automated processing

Article 22(1): The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]

The PPL does not explicitly refer to automated processing. However, the definition of 'database' covers data collected and intended for computer processing.





## 5.6. Right to data portability

Fairly inconsistent

In general terms, the PPL does not provide a comparable right to data portability as the GDPR. However, in some aspects, the right to inspection established in the PPL overlaps with requirements under the right to data portability in the GDPR.

| GDPR | PPL |
|---|---|

### Grounds for portability

Article 20(1): The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contrPPL pursuant to point (b) of Article 6(1); and
(b) the processing is carried out by automated means.

The PPL does not establish a right to portability, but it does cover the right to inspection (see section 4.4. above).

### Inform data subject of right

See Article 12(1) in section 5.1.

The PPL does not explicitly refer to the communication of rights to data subjects.

### Fees

See Article 12(5) in section 5.1. above.

The PPL does not explicitly establish a right to data portability.

### Response timeframe

See Article 12(3) in section 5.1. above.

The PPL does not explicitly establish a right to data portability.

### Format

See Article 20(1) above.

The PPL does not explicitly establish a right to data portability.

### Controller to controller

Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

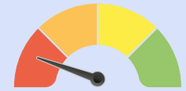
The PPL does not explicitly cover controller to controller transmissions for the data subject. However, Section 13A provided that, where the right to inspect information is exercised when information is not in the possession of the database owner: (1) The owner of a database who keeps it at the place of another person (in this section - the possessor)

| GDPR | PPL |
|---|---|
| **Controller to controller (cont'd)** | |
| | shall refer owner of the database the person making the request to the possessor, with his address, and order the possessor, in writing, to enable the person making the request the inspection; (2) Where the person making the request applies to the possessor first, the possessor shall inform him if he possesses information about him, and also the name and address of the owner of the database. |
| **Technically feasible** | |
| See Article 20(2) above. | The PPL does not explicitly establish a right to data portability. |
| **Exceptions** | |
| See Article 12(5) in section 5.1. above. | The PPL does not explicitly establish a right to data portability. |





# 6. Enforcement




## 6.1. Monetary penalties

Where the GDPR sets out levelled penalties for organisations violating its provisions, the PPL states which violations would constitute infringements of privacy and does not clarify specific corresponding monetary penalties. Furthermore, the PPL focuses on enforcement through prison sentences and civil claims.

| GDPR | PPL |
|---|---|
| **Provides for monetary penalties** | |
| The GDPR provides for monetary penalties. | The PPL does not provide for monetary penalties and Section 23H, on penalties, was repealed. However, the PPL does provide for civil claims and damages. |
| **Issued by** | |
| Article 58(2) Each supervisory authority shall have all of the following corrective powers:<br>[...] (i): to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case | Not applicable. |
| **Fine maximum** | |
| Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:<br>(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;<br>(b) the data subjects' rights pursuant to Articles 12 to 22;<br>(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;<br>(d) any obligations pursuant to Member State law adopted under Chapter IX;<br>(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).<br>(6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. | Not applicable. |

| GDPR | PPL |
|---|---|
| **Percentage of turnover** | |
| Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year. | Not applicable |
| **Mitigating factors** | |
| Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:<br>(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;<br>(b) the intentional or negligent charPPLer of the infringement;<br>(c) any PPLion taken by the controller or processor to mitigate the damage suffered by data subjects;<br>(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;<br>(e) any relevant previous infringements by the controller or processor;<br>(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;<br>(g) the categories of personal data affected by the infringement;<br>(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;<br>(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;<br>(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and<br>(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement. | Not applicable |





| GDPR | PPL |
|---|---|
| **Imprisonment** | |
| Not applicable. | Under Section 5, a person who wilfully infringes the privacy of another in any of the ways stated in Sections 2(1), (3) to (7) and (9) to (11) is liable to imprisonment for a term of five years.<br>Section 31A: (a) A person who commits any of the following is subject to imprisonment for a term of one year – (1) manages, possesses or uses a database in violation of the provisions of Section 8; (2) provides incorrect particulars in an application for registration of a database as required in Section 9; (3) fails to provide particulars or provides incorrect particulars in the notice accompanying a request to obtain information under Section 11; (4) fails to comply with the provisions of Sections 13 and 13A regarding the right to inspect information kept in a database or fails to correct information in accordance with the provisions of Section 14; (5) enables access to a database in violation of the provisions of Section 17A(a) or fails to provide to the Registrar documents or an affidavit in accordance with the provisions of section 17A(b); (6) fails to appoint a security supervisor in accordance with the provisions of Section 17B; (7) manages or possesses a database used for direct-mailing services, in violation of the provisions of Sections 17D to 17F; (8) delivers information in violation of the provisions of Sections 23B to 23E. (b) An offence under this section does not require proof of criminal intent or negligence.<br>Section 16: No person shall disclose any information obtained by him by virtue of his functions as an employee, manager or possessor of a database save for the purpose of carrying out his work or implementing the Law or under a court order in connection with a legal proceeding; where the request is made before a proceeding has been instituted, it shall be heard in the Magistrate's Court. A person who infringes the provisions of this section shall be liable to imprisonment for a term of five years. |
| **DPO liability** | |
| Not applicable. | The PPL does not explicitly refer to the liability of the security supervisor. |

# 6.2. Supervisory authority

Fairly consistent

The role of the PPA and the Registrar of Databases under the PPL is broadly similar to that of data protection authorities as envisioned by the GDPR. Both have advisory, investigatory and corrective powers, although the details of these powers differ and the PPA plays a very active additional role in the registration of databases.

| GDPR | PPL |
|---|---|
| **Provides for data protection authority** | |
| Article 51(1): Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority'). | The PPL details the role and responsibilities of the Registrar of Databases. |
| **Investigatory powers** | |
| Article 58(1): Each supervisory authority shall have all of the following investigative powers:<br>(a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks;<br>(b) to carry out investigations in the form of data protection audits;<br>(c) to carry out a review on certifications issued pursuant to Article 42(7);<br>(d) to notify the controller or the processor of an alleged infringement of this Regulation;<br>(e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;<br>(f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law. | Section 10: (c) The Registrar shall supervise compliance with the provisions of the PPL and the regulations thereunder.<br>(d) The Minister of Justice, with the approval of the Constitution, Law and Justice Committee of the Knesset, shall establish by order, a supervisory unit that will supervise the databases, their registration, and the information security therein; the unit shall be sized accordingly with the supervision needs.<br>(e) The Registrar shall head the supervisory unit, and shall appoint inspectors to carry out the supervision pursuant to the PPL; no person shall be appointed inspector unless he received the appropriate professional training in the field of computerisation and information security and exercising powers under the PPL, and the Israel Police did not object to his appointment for reasons of public safety. (e1) In carrying out his functions, an inspector may – (1) demand every relevant person to deliver to him information and documents relating to a database; (2) enter a place as to which he has reasonable belief that a database is being operated, search the place and seize objects, if he is convinced that doing so is necessary to ensure implementation of the PPL and to prevent violation of its provisions; the provisions of the Criminal Procedure (Arrest and Search) Ordinance [New Version], 5869 – 1969 (only available in Hebrew here) shall apply to an object that has been seized under this section; arrangements for entering a military installation or an installation of a security authority within its meaning in section 19(c) shall be determined by the Minister of Justice upon consultation with the minister in charge of the security authority, as the case may be; in this paragraph, 'object' includes computer material and output as defined in the Computers Law, 5765 – 1995 (only available to download in Hebrew here); (3) notwithstanding the provisions of paragraph (2), an inspector shall not enter a place that is used solely as a residence, other than pursuant to an order given by a judge of the Magistrate's Court. |
| **Corrective powers** | |
| Article 58(2): Each supervisory authority shall have all of the following corrective powers:<br>(a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;<br>(b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;<br>(c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;<br>(d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;<br>(e) to order the controller to communicate a personal data breach to the data subject;<br>(f) to impose a temporary or definitive limitation including a ban on processing;<br>(g) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such PPLions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19;<br>(h) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;<br>(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;<br>(j) to order the suspension of data flows to a recipient in a third country or to an international organisation. | Section 8(e): The Registrar may, for special reasons that shall be recorded, order the registration of a database that is exempt from registration pursuant to subsections (c) and (d); the said order, in which the Registrar shall set forth instructions as to managing and possessing the database until its registration, shall be served to the owner of the database.<br>Section 10(f): Where the possessor or owner of a database infringes any provision of the PPL or the regulations thereunder, or fails to comply with a request made to him by the Registrar, the Registrar may suspend the registration for a period that he shall determine or cancel the registration of the database in the Register, provided that prior to the suspension or cancellation the owner of the database was given the opportunity to be heard. |

| GDPR | PPL |
|---|---|

## Authorisation/ advisory powers

Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers:
(a) to advise the controller in accordance with the prior consultation procedure referred to in Article 36;
(b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
(c) to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;
(d) to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);
(e) to accredit certification bodies pursuant to Article 43;
(f) to issue certifications and approve criteria of certification in accordance with Article 42(5);
(g) to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);
(h) to authorise contrPPLual clauses referred to in point (a) of Article 46(3);
(i) to authorise administrative arrangements referred to in point (b) of Article 46(3);
(j) to approve binding corporate rules pursuant to Article 47.

Section 10: (a) Where an application for registration of a database is submitted –
(1) The Registrar shall register it in the register it, within 90 days from the day the application was submitted to him, unless he sees reasonable cause for believing that the database serves or is liable to serve illegal activities or as a cover for them, or that the information included within it was received, accumulated or collected in violation of the PPL or in violation of the provisions of any law;
(2) The Registrar may, if he is of the opinion doing so is appropriate for the actual operation of the database, record a different purpose than the one set forth in the application, record a number of purposes for the database, or order the submission of a number of applications under the application that was submitted;
(3) The Registrar shall not refuse to register the database pursuant to paragraph (1) and shall not exercise his powers pursuant to paragraph (2) unless he has given the applicant an opportunity to be heard.
(b) Repealed. (b1) Where the Registrar does not register the database within 90 days from the day the application was submitted to him, and does not notify the applicant of his refusal to register or of delay of the registration for special reasons that he shall record in his notice, the applicant may manage or possess the database although it is not registered.
(b2) Where the Registrar notifies the applicant of his refusal to register the database or of delaying the registration as stated in subsection (b1), the applicant shall not be allowed to manage or possess the database, unless the court rules otherwise. (b3) The Registrar shall delete the registration of a database from the Register if the owner of the database notifies him that the information in the database has been destroyed and verified the notice by affidavit; where a person other than the owner possesses the database, the notice shall also be verified by affidavit of the possessor.

## Tasks of authority

Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:
(a) monitor and enforce the application of this Regulation;
(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation

See Section 34 of the PPL above.





| GDPR | PPL |
|---|---|

## Tasks of authority

to processing. Activities addressed specifically to children shall receive specific attention;
(c) advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
(d) promote the awareness of controllers and processors of their obligations under this Regulation;
(e) upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;
(f) handle complaints lodged by a data subject, or by a body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;
(g) cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;
(h) conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
(i) monitor relevant developments, insofar as they have an impPPL on the protection of personal data, in particular the development of information and communication technologies and commercial prPPLices;
(j) adopt standard contrPPLual clauses referred to in Article 28(8) and in point (d) of Article 46(2);
(k) establish and maintain a list in relation to the requirement for data protection impPPL assessment pursuant to Article 35(4);
(l) give advice on the processing operations referred to in Article 36(2);
(m) encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
(n) encourage the establishment of data protection certification mechanisms and of data protection seals

Section 10(a)(3): The Registrar shall not refuse to register the database pursuant to paragraph (1) and shall not exercise his powers pursuant to paragraph (2) unless he has given the applicant an opportunity to be heard.
Section 12: (a) The Registrar shall keep a register of databases, which shall be open for inspection by the public.
(b) The register shall contain the particulars for registering the database as stated in Section 9.
(c) Notwithstanding the provisions of subsections (a) and (b), in a database of a security authority, the particulars stated in Section 9(b)(3), (4) and (5) shall not be open to inspection by the public.

| GDPR | PPL |
|---|---|

## Tasks of authority (cont'd)

and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);
(o) where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);
(p) draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
(q) conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
(r) authorise contrPPLual clauses and provisions referred to in Article 46(3);
(s) approve binding corporate rules pursuant to Article 47;
(t) contribute to the PPLivities of the Board;
(u) keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and
(v) fulfil any other tasks related to the protection of personal data.

## Annual report

Article 59: Each supervisory authority shall draw up an annual report on its PPLivities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.

Section 10A: No later than the first of April every year, the Protection of Privacy Council shall submit to the Constitution, Law and Justice Committee of the Knesset a report that the Registrar shall prepare on the enforcement and supervisory activities in the year preceding submission of the report, along with the Council's comments





# 6.3. Civil remedies for individuals

**Fairly consistent**

Both the GDPR and the PPL provide for comprehensive remunerations and damages to be paid to injured parties and in the event of civil wrongs.

| GDPR | PPL |
|---|---|

## Provides for claims/ cause of action

Article 79: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

Section 4: An infringement of privacy is a civil wrong, and the provisions of the Civil Wrongs Ordinance (New Version) shall apply to it subject to the provisions of the PPL.

## Material and non-material damage

Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

The PPL does not directly address types of damages, and it only stipulates for statutory damages (see Section 29A of the PPL below).

## Mandate for representation

Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is PPLive in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.

The PPL does not explicitly refer to a mandate for representation.

## Specifies amount for damages

Not applicable.

Section 29A: (a) The court may order a person who has been convicted under Section 5 to pay the injured person statutory damages, that will not exceed 50,000 new shekels [approx. €13,000]; an order for damages under this subsection shall be regarded as a ruling of the same court in a civil proceeding of the entitled against the person obliged. (b) (1) In a civil wrong-doing proceeding under Section 4,

| GDPR | PPL |
|---|---|

## Specifies amount for damages (cont'd)

| | |
|---|---|
| | the court may order that the defendant shall pay the plaintiff statutory damages that will not exceed 50,000 new shekels. (2) In a proceeding under paragraph (1) in which it was proven that the infringement on privacy was made with intent to cause harm, the court may order that the defendant shall pay the plaintiff statutory damages that will not exceed double the amount in that paragraph. (c) A person shall not be awarded statutory damages under this section, for the same infringement on privacy, more than once. (d) The amounts in this Section shall be updated at the 16th of each month, in accordance with the rate of change in the new index compared with the basic index; in this regard – 'index' – the consumer price index as published by the Central Bureau of Statistics; 'the new index' – the index of the month which proceeded the month of update; 'the basic index' – the index of May 2007. |

## Processor liability

| | |
|---|---|
| Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has PPLed outside or contrary to lawful instructions of the controller. | The PPL does not directly address processor liabilities. Sections 30 and 31 of the PPL define liabilities in relation to publications in newspapers and printing/distribution respectively. |

## Exceptions

| | |
|---|---|
| Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage. | Section 6: No right to bring a civil or criminal action under the PPL shall accrue through an infringement of no real significance. |