# For the purpose of this law:

**“Information security”** - Protection of the integrity of personal information or protection of personal information from processing without legal authorization;

**“Person”** - For the purposes of sections 2, 7, 13, 14, 15a, 17b, 17c, 17b1, 17b2, 17f, 17g, 23a, 23b, 23b, 23f, and 25, as well as for the definitions of “direct mailing," “database," “biometric identifier," “personal information," and “information of special sensitivity” - excluding corporations;

**“Controller”** of a database - One who determines, alone or together with another, the purposes of processing the information in the database or a body that is or an official in it authorized by law to process information in a database;

**“Direct mailing”** - Personal approach to a person, based on their belonging to a population group, determined by one or more characteristics of people whose names are included in a database;

**“Late fees”** and **“shekel interest”** - As defined in the Interest and Linkage Ruling Law, 1961;

**“Consent”** - Informed consent, explicitly or implicitly;

**“Constitution Committee”** - The Constitution, Law and Justice Committee of the Knesset;

**“Computer material," “computer,"** and **“output”** - As defined in the Computer Law;

**“Law for Regulating Security in Public Bodies”** - Law for Regulating Security in Public Bodies, 1998;

**“Freedom of Information Law”** - Freedom of Information Law, 1998;

**“Computer Law”** - Computer Law, 1995;

**“Detention Law”** - Criminal Procedure Law (Enforcement Powers - Arrests), 1996;

**“Object”** - As defined in the Arrest and Search Ordinance;

**“Database”** - A collection of personal information items processed by digital means, except for one of the following:

A collection for personal use that is not for business purposes;

A collection that includes only name, address, and contact details, for 100,000 people or less, which does not in itself teach about additional personal information regarding the people whose names are included in it, provided that the owner of the collection or a corporation under its control does not have another collection containing other information items regarding those people;

**“Biometric identifier”** - Biometric data used to identify a person or verify their identity, or a biometric means from which such data can be derived; For the purpose of this definition, “biometric” - a unique human, physiological or behavioral characteristic that can be computationally measured;

**“Holder,"** regarding a database - One who permanently possesses a database and is authorized to use it;

**“Holder,"** regarding a database - An external entity to the controller of the database that processes information for them;

**“Personal Information”** - Data relating to an identified or identifiable person; For the purpose of this definition, “identifiable person” means one who can be identified with reasonable effort, directly or indirectly, including by means of an identifying detail, such as name, ID number, biometric identifier, location data, online identifier, or one or more details relating to their physical, health, economic, social or cultural status;

**“Information of Special Sensitivity”** - Any of the following:

Personal information about a person’s family privacy, personal intimacy, and sexual orientation;

Personal information relating to a person’s health condition, including medical information as defined in the Patient Rights Act, 1996;

Personal information that is genetic information as defined in the Genetic Information Law, 2000;

Personal information that is a biometric identifier used or intended to be used to identify a person or verify their identity in a computerized manner;

Personal information about a person’s origin;

Personal information about a person’s criminal history;

Personal information about a person’s political opinions, religious beliefs, or worldview;

Personal information that is a personality assessment conducted by a professional who, as a matter of practice, gives their opinion on a person’s personality, or conducted by means intended to evaluate essential personality characteristics, including character traits, intellectual ability, and ability to function at work or in studies;

Personal information that is location data and traffic data, as defined in the Criminal Procedure Law (Enforcement Powers - Communications Data), 2007, created by an authorized provider as defined in that law, regarding a person, and data about a person’s location that can teach about information under paragraphs (1) to (7) and (11);

Personal information on a person’s salary data and financial activity;

Personal information subject to a statutory duty of confidentiality;

Other personal information determined by the Minister of Justice, with the approval of the Constitution Committee, in the Second Schedule, provided that it is personal information in a database located in Israel that was transferred to it from outside the state borders, and that in the place from which it was transferred, special legal provisions apply to personal information of its type in relation to the law applicable to other personal information;

**“Database Manager”** - A controller of a database, and regarding a public body as defined in section 23 - the general manager of a body that owns or holds a database or someone the general manager authorized to manage the database;

**“Document”** - including output;

**“Inspector”** - one who was authorized according to the provisions of section 23i;

**“Registry”** - the database registry as defined in section 12;

“System data” - Data about the possession and management of personal information and a database and about their use, provided that they do not include personal information;

“Processing," “Use” - Any operation performed on personal information, including receiving it, collecting it, storing it, copying it, viewing it, disclosing it, exposing it, transferring it, delivering it or providing access to it;

“Arrest and Search Warrant” - Criminal Procedure Ordinance (Arrest and Search) [New Version], 1969;

“Publication” - As defined in Section 2 of the Prohibition of Defamation Law, 1965; “Photography” - including filming.

“Head of the Authority” - The person appointed by the government to head the Privacy Protection Authority and supervise the protection of personal information in databases according to the provisions of this law;

“The Authority," “Privacy Protection Authority” - The Privacy Protection Authority established and operating according to Government Decisions No. 4660 of January 19, 2006, No. 4820 of June 28, 2012, No. 3019 of September 7, 2017 and Government Decision No. 1890 of October 2, 2022, the text of which is provided in the First Addendum;

“Use” - including disclosure, transfer and delivery.

“Use” - (deleted)

“Direct mailing services” - Providing direct mailing services to others by transferring lists, labels or data by any means;

“Data integrity” - The identity of the data in a database to the source from which it was drawn, without being changed, transmitted or destroyed without legal permission.

### [Replacement] Registration of a database and its use

8. (a) No person shall manage or hold a database required to be registered under this section, unless one of the following applies:

8. (a) In this section, “processing” - except for accidental and good faith storage.

(b) No person shall process personal information in a database except for the purpose legally determined for the database.

(c) No person shall process personal information from a database without authorization from the controller of the database or in excess of such authorization.

(d) (1) A controller of a database shall not process personal information in a database and shall not allow another to process such information on his behalf, if the personal information included in the database was created, received, accumulated or collected in violation of the provisions of this law or any other law regulating information processing;

(2) If personal information was provided to a database controller from another source, and the controller did not know and should not have known that the source acted unlawfully, the database controller shall not be liable under this subsection for processing personal information performed before he knew or should have known as stated;

(3) The provisions of paragraph (1) shall not apply to minor violations of law under the circumstances, and with respect to personal information provided as stated in paragraph (2), even if the controller knew or should have known.

### Management of a Database and Lawful Processing of Personal Information

8a. (a) (1) A database must be registered if one of the following applies:

Its main purpose is collecting personal information for transfer to others as a business or for compensation, including direct mailing services, and the database contains personal information on more than 10,000 individuals;

The controller of the database is a public body as defined in paragraph (1) of the definition of “public body” in section 23, unless the database contains personal information only about employees of the public body;

A controller of a database shall not process personal information in a database required to be registered and shall not allow another to process such information on its behalf, unless the database is registered in the registry; for this purpose, a database shall be considered registered if the controller of the database submitted an application for registration of the database according to the provisions of section 9 and the period specified in section 10(a)(1) has elapsed, without the head of the Authority notifying the applicant of refusal to register the database or suspension of the registration of the database;

The head of the Authority may exempt a database required to be registered from the registration requirement under paragraph (1), if convinced that registration is not necessary to ensure compliance with the provisions of this law regarding the database; such notice shall be delivered to the controller of the database and published on the Authority’s website.

(b) (1) If the number of individuals about whom there is information of special sensitivity in a database that is not required to be registered under subsection (a)(1) exceeds 100,000, the controller of the database shall notify the Authority, within 30 days of the occurrence, of the identity of the controller, their address and contact details, the identity of the privacy protection officer - if their appointment is required under section 17b1, and their contact details, and shall provide the Authority with a copy of the database definitions document required to be prepared in accordance with regulations under sections 17(b) and 36;

(2) The controller referred to in paragraph (1) shall notify the Authority, within 30 days of the change or cessation of activity, as applicable, of any change in the identity of the controller or the identity of the privacy protection officer and their contact details, of any change requiring updating of the database definitions document in accordance with regulations under sections 17(b) and 36, and of the cessation of the database’s activity;

(3) The Minister of Justice may establish provisions regarding the methods of notification under this subsection, and may, with the approval of the Constitution Committee, exempt certain types of databases from the notification requirement.

**Information or types of controlling owners.**

(c) The provisions of this section shall not apply to a database that contains only information published to the public by lawful authority or made available for public inspection by lawful authority.

### Obligation of registration or notification

9. (a) An application for registration of a database shall be submitted to the head of the Authority.

(b) An application for registration of a database shall specify:

The identity of the controlling owner of the database, the database holder and the database manager, and their addresses in Israel and contact details, and the identity of the privacy protection officer and their contact details;

1a) The type of service provided by the database holder to its controlling owner;

2) The purposes for establishing the database and the purposes for which the information is intended;

3) The types of information to be included in the database;

4) Details regarding the transfer of information outside the state borders;

5) Details regarding the regular receipt of information from a public body as defined in section 23, the name of the public body providing the information and the nature of the information provided, except for details provided with the consent of the person about whom the information is about.

(c) The Minister of Justice, with the approval of the Constitution Committee, may prescribe in regulations additional details to be specified in the registration application.

(d) The controlling owner of a database shall notify the head of the Authority of any change in any of the details specified in subsection (b) or under subsection (c) and of the cessation of operation of the database.

### Application for registration

10. (a) When an application for registration of a database is submitted:

The head of the Authority shall register it in the registry within 60 days from the day the application was submitted, unless they had reasonable grounds to believe that the database serves or may serve for illegal activities or as a cover for them, or that the personal information contained in it was created, received, accumulated or collected in violation of this law or in violation of any law, however if the head of the Authority demanded additional information and details from the applicant, the period of time until such information and details are submitted shall not be included in the aforementioned period;

The head of the Authority may register a different purpose than the one specified in the application, register multiple purposes for the database, or instruct on the submission of several applications instead of the one submitted, or register the database as several separate databases, all if they are convinced that this suits the actual activity of the database;

The head of the Authority shall not refuse to register the database under paragraph (1) and shall not exercise their powers under paragraph (2), except after giving the applicant an opportunity to present their arguments.

(Canceled)

)ב(1 If the Registrar did not register the database within 90 days from the day the request was submitted, and did not notify the applicant of refusal to register or suspension of registration for special reasons to be detailed in the notice - the applicant may manage or hold the database even though it is not registered.

)ב(2 If the Registrar/Head of Authority notified the applicant of refusal to register the database, or of suspension of registration as stated in subsection (b)(1), the applicant shall not be permitted to manage or hold the database, process personal information in the database, or allow another to process personal information for him, unless the court determined otherwise.

)ב(3 The Registrar/Head of Authority shall delete the registration of a database from the ledger/registry, if the database owner/controller notified him that the information in that database was destroyed or transferred to another registered database and no longer exists, or that the database is no longer required to be registered, and verified this notice by affidavit.

)ג( The Registrar shall supervise the fulfillment of the provisions of this law and regulations pursuant to it.

### Powers of the Registrar/Head of Authority in connection with database registration

)ד( The Minister of Justice, with approval of the Constitution, Law and Justice Committee of the Knesset, shall establish by order a supervisory unit that will oversee databases, their registration and information security; the size of the unit shall be adapted to supervisory needs.

)ה( The Registrar shall head the supervisory unit, and shall appoint inspectors for carrying out supervision under this law; only a person who has received appropriate professional training in computing and information security and exercising powers under this law, and the Israel Police has not expressed objection to his appointment for reasons of maintaining public security, shall be appointed as an inspector.

)ה(1 For the purpose of carrying out his duties, an inspector may -

Demand any relevant person to provide information and documents relating to a database;

Enter a place where there is reasonable grounds to believe a database is operated, conduct a search there and seize an object, if convinced it is necessary to ensure implementation of this law and to prevent violation of its provisions; provisions of the Criminal Procedure Ordinance (Arrest and Search) [New Version], 1969 shall apply to an object seized under this section; procedures for entering a military facility or facility of a security authority as defined in section 19(c) shall be determined by the Minister of Justice in consultation with the minister responsible for the security authority, as applicable; in this paragraph, “object” - including computer material and output as defined in the Computers Law, 1995;

Notwithstanding the provisions of paragraph (2), shall not enter a place as stated that serves solely for residence, except by warrant from a Magistrate’s Court judge.

Right to review personal information

(a) Every person has the right to inspect by himself, or by his representative authorized in writing or by his guardian, the personal information about him held in a database.

(b) A controller of a database will allow the review of personal information, at the request of a person as stated in subsection (a) (hereinafter – the applicant), in Hebrew, Arabic or English.

Database Register

12. (a) The head of the authority shall maintain a registry of databases that will be open to the public's inspection and will enable the search of its details.

(b) The registry shall contain the details for registering the database as stated in section 9, except for the name of the Privacy Protection Officer.

(c) Notwithstanding the provisions of subsections (a) and (b), in the database of a security authority, the details specified in section 9(b)(1)(a) and (3)-(5) shall not be open to public inspection.

Obligation to request information

11. A request to a person for personal information for the purpose of holding or processing it in a database will be accompanied by a notice that will be noted in it:

If the person has a legal obligation to provide the information, or the disclosure of the information depends on his will and consent and what is the result of the disagreement;

the purpose for which the information is sought;

(2A) the name of the controller of the database, and ways of communicating with him;

(3) To whom the information and the purposes of delivery will be provided.

(4) The existence of the right to review personal information under section 13 and the right to request correction of the personal information under section 14.

Privacy Protection Report

10A. Not later than April 1 of each year, the Privacy Protection Council shall submit to the Knesset Constitution, Law and Justice Committee a report prepared by the Registrar on enforcement and supervision activities in the year preceding the submission of the report, together with the Council's comments.

(f) If a database controller or database holder violates the provisions of this Law or the regulations thereunder, or fails to comply with a requirement referred to him by the head of the authority, the head of the authority may suspend the validity of the registration for a period to be determined or cancel the registration of the database in the registry, if he is convinced that this is required under the circumstances, provided that prior to the suspension or cancellation, the controlling shareholder of the database or the holder of the database was given an opportunity to voice his claims.

(g) The law of the Registrar and anyone acting on his behalf as a civil servant.

Database owner/controller:

(c) may not provide the applicant with personal information relating to his medical or mental condition if, in his opinion, the information may cause serious harm to the physical or mental health of the applicant or endanger his life; in this case, the owner of the database/control of the database will provide the information to a doctor or psychologist on behalf of the applicant.

(1c) The provisions of this section do not require the disclosure of personal information contrary to the confidentiality established under any law, unless the applicant is a person for whose benefit the confidentiality is intended.

In this subsection, "law" includes halachic law.

(d) The manner, conditions and payment for exercising the right to view personal information will be determined in the regulations.

(e) The provisions of this section and section 13A shall not apply —

on a database of a security authority within the meaning of section 19(c); (1A) on a database of the Israel Prison Service;

On a database of a tax authority within the meaning of the Tax Law Amendment Law (Exchange of Information between Tax Authorities), 5727-1967;

When the security of the state, its foreign relations or legislative provisions require that information about it not be disclosed to a person.

On a database of entities that 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 Knesset Foreign Affairs and Defense Committee, has determined that it includes information that the security of the State or its foreign relations requires not to be disclosed (hereinafter – confidential information), provided that a person who wishes to review the personal information about him held in that database will be entitled to review information that is not confidential information.

A database on investigations and law enforcement of an authority authorized to investigate an offense by law, which the Minister of Justice determined by order, with the approval of the Knesset's Constitution, Law and Justice Committee.

On a database established pursuant to section 28 of the Prohibition of Money Laundering Law, 5760-2000.

13A. Without derogating from the provisions of section 13 –

The owner of a database/control of a database, who holds it with another (in this section – the holder), shall refer the applicant to the holder, stating his address, and instruct the holder, in writing, to allow the applicant to peruse;

If the applicant first contacts the holder, the holder will inform him if he holds personal information about him, as well as the name and address of the owner of the database/control of the database.

### Review of personal information that is not held by the database owner / controller

(a) A person who has reviewed the personal information about him and found it to be incorrect, incomplete, unclear or out of date, may contact the owner of the database/control of the database, and if he is a foreign resident – the owner of the database, with a request to correct or delete the personal information.

(b) If the controller of the database agrees to a request as mentioned in subsection (a), they shall make the required changes to the personal information in their possession and notify anyone who received the personal information from them within the period specified in the regulations.

(c) If the controller of the database refuses to fulfill a request as mentioned in subsection (a), they shall notify the requester in the manner and way specified in the regulations.

(d) A processor is obligated to correct information, personal information, if the controller of the database agreed to the requested correction or if a court ordered the correction.

### Correction of Personal Information

Regarding the refusal of a database controller to allow access as mentioned in section 13 or section 13a and regarding a notice of refusal as mentioned in section 14(c), the information requester may file a claim to the court in the manner and way specified in the regulations.

### Court Claim

15a. (a) If a database controller or processor violates any of the provisions detailed below, the court may award, for that violation, damages that are not dependent on harm (in this section - exemplary damages), in an amount not exceeding 10,000 New Israeli Shekels:

Regarding a database controller - if the database is required to be registered according to the provisions of section 8a - processed personal information in a database without being registered, contrary to the provisions of that section, provided that a person to whom the personal information relates approached the controller with a demand to register the database, and 90 days have passed since their approach;

Approached a person to obtain personal information for processing in a database according to section 11 or 23d(a) without providing notice as required by that section, provided that such a person approached the controller with a demand to notify them as stated, and 30 days have passed since their approach;

Regarding a database controller - did not allow a person who requested to view personal information about them held in the database to view the information, contrary to the provisions of sections 13 or 13a, at the time and in the manner specified in the regulations under section 13;

Agreed to a request to correct or delete personal information that is not accurate, complete, clear, or up-to-date, but did not make the required changes to the personal information in their possession, or did not notify anyone who received the personal information from them within the period specified in the regulations under section 14(b), contrary to the provisions of that section;

Did not notify a person who requested to correct or delete personal information about them, which is not accurate, complete, clear, or up-to-date, of their refusal, in the manner and way specified in the regulations under section 14(c), contrary to the provision of that section;

**Regarding the controller of a database:** Did not notify the head of the Authority about regularly receiving personal information stored in a database according to section 23d(c), provided that the person to whom the personal information relates approached the controller with a request to notify as stated, and 30 days have passed since their request.

**Exemplary damages**

(b) When determining the amount of exemplary damages, the court shall consider, among other things, the following considerations, and shall not consider the amount of damage caused to the injured party as a result of the violation:

Encouraging the plaintiff to exercise their rights;

The scope and severity of the violation;

The behavior of the violator, their personal circumstances and financial ability, as well as additional enforcement measures or additional payment imposed on the violator for the same violations.

(c) The provisions of this section do not derogate from the possibility of conducting criminal proceedings if the violation also constitutes a criminal offense, from the possibility of using authority under Chapter D3, or from the plaintiff’s right to claim any other remedy under the Torts Ordinance [New Version], for the same violation; however, a person shall not receive exemplary damages under this section, for the same act or omission, more than once.

**Confidentiality**

A person shall not disclose personal information that came to them by virtue of their position as an employee, manager or holder of a database, except for the purpose of performing their work or for the implementation of this law or by court order in connection with legal proceedings; if the request was submitted before the start of the proceedings, the request will be discussed in the Magistrate’s Court. Anyone violating the provisions of this section is liable to 5 years imprisonment.

**Responsibility for information security**

(a) The controller of a database and the holder of a database, each of them is responsible for the security of the information in the database.

(b) (1) The Minister of Justice, with the consent of the Prime Minister and with the approval of the Constitution Committee, may establish regulations regarding the responsibility for information security set forth in subsection (a) and in section 17b(b), including its scope and the obligations included therein, as well as regarding the ways of securing said information, inter alia in these matters:

Physical and logical protection of the database;

Management procedures and work rules in and related to the database, including regarding the determination of restrictions on employee access to information;

In regulations under paragraph (1), different provisions may be established for databases with different characteristics;

Regulations under paragraph (1) that will apply to bodies listed in items 2 and 3 in the First Schedule to the Law for Regulating Security in Public Bodies - will also be enacted in consultation with the Minister of Defense.

**Cancellation**

### Holds databases of different owners

**17A.** (a) The holder of databases of different owners shall ensure that access to each database shall be granted only to those who have been expressly authorized to do so by written agreement between him and the owner of that database.

(b) A holder in possession of at least five databases that are required to be registered pursuant to section 8 shall submit to the Registrar, every year, a list of the databases in his possession, indicating the names of the database owners, an affidavit stating that for each of the databases those entitled to access the database have been determined by an agreement between him and the owner, and the name of the security officer as stated in section 17B.

### Information Security Officer

**17B.**(a) The entities listed below must appoint a person with appropriate training to be in charge of information security (hereinafter – the Commissioner):

Has control of five databases that require registration or notification under section 8A or holds five such databases;

a public body as defined in article 23;

Bank, insurance company, company engaged in rating or evaluating credit.

(b) Without derogating from the provisions of section 17, the Information Security Officer shall be responsible for information security in the databases held by the entities as stated in subsection (a).

(c) No person who has been convicted of an offense involving disgrace or a violation of the provisions of this Law shall be appointed as an information security officer.

**17B1.** (a) The following entities must appoint a Privacy Protection Officer:

A controller of a database that is a public body as defined in section 23 or holds such a database, except for a security body as defined in section 23K;

A controller of a database whose main purpose is to collect personal information for the purpose of providing it to another as a way of business or in exchange, including direct mail services, and the database contains personal information about more than 10,000 people;

A controller of a database or a database holder whose main occupations include information processing activities or involve such activities, which, in view of their nature, scope or purpose, require ongoing and systematic monitoring of persons, including monitoring or systematically tracing the behavior, location or actions of a person, on a significant scale, including an authorized supplier providing radio and mobile phone service under the Communications Law (Telecommunications and Broadcasting), 5742-1982, and an online search service provider or a person whose primary business involves these activities;

The controller of a database or the processor of a database whose main business includes processing highly sensitive information on a significant scale, including a banking corporation as defined in the Banking (Customer Service) Law, 1981, an insurer as defined in the Financial Services Supervision (Insurance) Law, 1981, a general hospital as defined in the Public Health Ordinance, 1940, and a health fund as defined in the National Health Insurance Law, 1994.

(b) For the purposes of paragraphs (3) and (4) of subsection (a) - processing of information on a significant scale shall be, inter alia, with regard to the number of individuals whose information is processed, their proportion in a certain population, the scope of information, its quantity and range of types of processed information, the duration and frequency of processing operations, the duration of information retention, and the geographical area of processing operations.

### Obligation to Appoint a Privacy Protection Officer

17b.(2a) The Privacy Protection Officer shall act to ensure compliance with the provisions of this law by the controller of the database or the processor of the database, and to promote privacy protection and information security in databases, including -

Serve as a professional authority and knowledge center, advise the management of the body in which they perform their role and its employees, prepare a training program and supervise its implementation;

Prepare a plan for ongoing monitoring of compliance with the provisions of this law regarding databases, ensure its implementation by the controller of the database or the processor of the database, report to the management of the body in which they perform their role on their findings and propose suggestions for correcting deficiencies;

Ensure the existence of an information security procedure and a database definitions document, the preparation of which is required in accordance with regulations under sections 17b and 36, to be submitted for approval to the management of the body in which they perform their role;

Ensure handling of inquiries from individuals whose personal information is in the database, regarding the processing of such information or the exercise of their rights under this law, including requests to review personal information or correct it; The contact details of the Privacy Protection Officer shall be published to the public in an accessible and simple manner;

Serve as the contact person of the body in which they perform their role with the Authority.

(b) The controller of the database or the processor of the database, as applicable, shall provide the Privacy Protection Officer with the conditions and resources necessary for the proper fulfillment of their role and ensure that they are appropriately involved in all matters relating to privacy protection laws.

### Duties of the Privacy Protection Officer

(c) The privacy protection officer shall report directly to the general manager of the data controller or the data processor, as applicable, or to an employee who reports directly to the general manager of the controller or processor, as applicable.

17b. (3a) The privacy protection officer shall possess the knowledge and qualifications necessary to properly fulfill their role, including in-depth knowledge of privacy protection laws, appropriate understanding of technology and information security, and familiarity with the activities and objectives of the organization in which they serve, taking into account the nature, circumstances, scope, and purposes of the data processing.

(b) The privacy protection officer may be someone who is not an employee of the organization in which they fulfill their role.

(c) The privacy protection officer shall not hold an additional position or be subordinate to an officer in the organization where they fulfill their role or in another organization, if such position or subordination may create a conflict of interest in fulfilling their duties under this law.

### Qualifications of the Privacy Protection Officer and Fulfillment of Role

### Definitions

17c. In this section –

“Direct mailing” – personal approach to an individual, based on their belonging to a population group, determined by one or more characteristics of individuals whose names are included in a database;

“Approach” – including in writing, print, telephone, fax, computerized means, or other medium;

“Direct mailing services” – providing direct mailing services to others by transferring lists, labels, or data by any means.

### Direct Mailing

17d. A data controller or data processor shall not process personal information in a database used for direct mailing services unless it is registered in the registry and one of its registered purposes is mailing services.

### Indication of Information Source

17e. A data controller or data processor shall not process personal information in a database used for direct mailing services unless they have a record indicating the source from which they received each data set used for the database and the date of receipt, as well as to whom they transferred any such data set.

17f. (a) Every approach in direct mailing shall clearly and prominently contain –

An indication that the approach is direct mailing, along with the registration number of the database used for direct mailing services in the database registry;

A notice of the recipient’s right to be removed from the database as stated in subsection (b), along with the address to which requests for removal should be sent;

The identity and address of the controller of the database containing the personal information based on which the referral was made, and the sources from which the controller obtained this information.

### Deletion of information from a database used for direct mailing

(b) Every person has the right to demand, in writing, from the controller of a database used for direct mailing, that personal information relating to them be deleted from the database.

(c) Every person has the right to demand, in writing, from the controller of the database used for direct mailing services or from the controller of the database containing the information based on which the referral was made, that personal information relating to them not be transferred to a person, a type of persons, or specific individuals, all for a limited or permanent period.

(d) If a person notifies the controller of the database of their demand as stated in subsections (b) or (c), the controller shall act in accordance with the demand and notify the person, in writing, that they have acted accordingly.

(e) If the controller of the database does not notify as stated in subsection (d) within 30 days from the day of receiving the demand, the person to whom the information relates may apply to the Magistrate’s Court in the manner prescribed in regulations, in order for it to instruct the controller of the database to act as stated.

(f) The rights under this section of a deceased person registered in a database are also granted to their spouse, child, parent, or sibling.

### Cancellation

17z. The provisions of this section shall apply to information concerning a person’s private affairs, even if not within the definition of information, as they apply to information.

### Applicability to information

### Section C: The Privacy Protection Authority

17t.(1a) The head of the Authority shall supervise the fulfillment of the provisions of this law and the regulations thereunder regarding databases.

(b) The law applicable to those acting on behalf of the head of the Authority is the same as that of a state employee, unless otherwise specified in this law.

(c) The Authority shall publish its procedures regarding the exercise of its powers on its website; however, details that are information that a public authority is prevented from disclosing under section 9(a) of the Freedom of Information Law shall not be published, and the Authority may refrain from publishing details that are information that a public authority is not obligated to disclose under section 9(b) of the said law.

(d) Notice of the appointment of the head of the Authority shall be published in the Official Gazette.

### The Privacy Protection Authority

17t.(2a) At the request of a controller of a database or a processor of a database, or someone who is about to become one of these, the Authority shall provide a preliminary opinion regarding the compliance of the database with the requirements of this law or the provisions thereunder regarding the processing of information in the database (in this law - preliminary opinion).

(b) A request for a preliminary opinion shall include the purpose of the request and all the facts required for providing the opinion, along with the relevant documents.

(c) A preliminary opinion shall be given within 60 days from the date of receiving the request as mentioned in subsection (b) or from the date of submission of the relevant documents, whichever is later; the head of the Authority may extend the deadline under special circumstances. If the Authority decides not to give a preliminary opinion, it shall notify the applicant within 45 days from the aforementioned date.

### Preliminary Opinion

(d) The Authority may publish a preliminary opinion with the consent of the applicant; if the applicant does not agree to the publication of the preliminary opinion, the Authority may publish it without details that could identify the applicant.

(e) The head of the Authority shall establish a procedure, which will be published on the Authority’s website, regarding the methods of submitting requests for preliminary opinions and circumstances in which opinions will not be given for requests of the following types:

A request for which the Authority’s position has been published in the past or for which there is a clear ruling;

A request whose scope and implications are limited to the applicant’s matter in relation to the significant resource allocation that handling it would require;

A request that is theoretical or academic in nature;

A request tainted by lack of good faith;

A request related to pending proceedings, including supervision, investigation, or criminal enforcement proceedings, under this law;

A request whose handling would require unreasonable resource allocation.

(3a) The head of the Authority shall prepare by June 1st of each year a report on the actions taken by the Authority to implement the provisions of this law in the year preceding the preparation of the report, including enforcement and supervision actions (in this section - report on the activities of the Privacy Protection Authority); The Privacy Protection Council shall submit the report, along with its comments, no later than July 1st of each year, to the Constitution Committee.

(b) A report on the activities of the Privacy Protection Authority shall include, among other things, information as detailed below, broken down by government ministries, other public bodies, and private entities:

The number of requests for preliminary opinions submitted to the Authority and the number of opinions given;

The number of requests for registration of databases submitted under section 8a(a) and the number of requests refused or databases whose registration was suspended under section 10(a), and the reasons for refusal or suspension;

The number of databases required to be registered under section 8a(a), which were granted exemption from registration obligation;

The number of databases whose registration was suspended or canceled under section 10(f);

The number of notifications about databases submitted to the Privacy Protection Authority according to Section 8a(b) and the number of controllers or processors of said databases that underwent supervision or administrative inquiry in the year following the submission of the notification;

The number of complaints filed with the Authority against database controllers or processors, regarding violations under this law;

The number of horizontal supervisions conducted according to Section 23(17);

The number of administrative inquiry procedures opened according to Section 23(12)(a), and how many of them resulted in a decision to conduct an investigation instead of an inquiry procedure, according to Section 23(16)(b);

The number of search and seizure warrants or computer material access requests made to the court according to Section 23(14)(a) and the number of cases in which the warrant was granted;

The number of complaints filed with the head of the Authority against an external expert according to Section 23(18)(h), and how many of them were found justified;

The number of orders to cease violation given according to Section 23(25), categorized by types of violations, how many of them were appealed, and how many appeals were fully or partially accepted;

The number of administrative warnings given according to Section 23(36), how many of them had cancellation requests filed according to Section 23(37), and what were the results of the requests;

The number of cases in which a violator was notified of the possibility to submit a letter of commitment and deposit a guarantee instead of imposing a monetary sanction according to Section 23(39), and in how many cases the violator submitted a letter of commitment and deposited a guarantee according to Section 23(40)(c);

### Report on the Privacy Protection Authority’s Activities and Reporting to the Constitution Committee

The total monetary sanctions imposed according to Section 23(26), the average amount of monetary sanction imposed, the highest sanction amount imposed, and the lowest sanction amount imposed;

The number of cases in which a violator requested to exercise the right to a hearing according to Section 23(28), and the average time frame for exercising the right to a hearing;

The number of cases in which a charge notice was issued but no monetary sanction was imposed, and the reasons for non-imposition;

The number of cases in which the monetary sanction was reduced according to Section 23(31) and the Fifth Addendum, in how many of them the sanction amount was reduced because it exceeded the maximum allowed percentage of the body’s transaction turnover, in how many - because it exceeded the sanction ceiling for a micro or small business according to that addendum, and in how many - because a privacy protection officer was appointed in bodies listed in Section 17b(1a)(3) and (4);

The number of repeated violations that occurred, how many of them occurred after an administrative warning was given to the violator according to Section 23(36), and how many of them occurred after submitting a letter of commitment and depositing a guarantee according to Section 23(40);

Number of ongoing violations that occurred; (20) Number of appeals filed against decisions of the Authority head to impose financial sanctions, administrative warnings, or letters of commitment and security deposit according to Chapter D3, in how many of them the execution of the decision was delayed, and in how many the appeal was accepted; (21) Number of cases where financial sanctions imposed on corporations were not published and number of cases where financial sanctions given to individuals or corporations were published as stated in Section 23mo; (22) Number of requests submitted for cessation orders according to Section 23mat and in how many of them such orders were issued; (23) Data on criminal enforcement carried out by the Authority, including the number of investigations opened by an investigator, number of indictments filed following said investigations, categorized by offense sections, in how many of them the proceeding ended in conviction, and what was the punishment in each case; (24) Number of requests for approval to exercise the authority of the Authority head, inspector, or investigator submitted to the chairman of the Central Elections Committee or the chairman of the Regional Elections Committee, as applicable, in accordance with Section 23nat; how many of them were accepted and in how many conditions were set. (c) To the report on the activities of the Privacy Protection Authority according to subsection (a), the Authority head shall attach a report on the number of lawsuits filed in court for compensation without proof of damage according to Section 15a and the case numbers of said lawsuits, according to information provided by the Courts Administration.

### Definitions

In this chapter and in Chapter D:

“Data security” - Protection of data integrity, or protection of information from exposure, use or copying, all without lawful permission;

“Database” - A collection of data, held by magnetic or optical means and intended for computerized processing, except - (1) A collection for personal use not for business purposes; or (2) A collection that includes only name, address and contact details, which in itself does not create a characterization that infringes on the privacy of the individuals whose names are included in it, provided that the collection owner or a corporation under its control does not have an additional collection;

“Information” - Data on a person’s personality, personal status, intimacy, health condition, economic situation, professional qualifications, opinions and beliefs;

“Sensitive information” - (1) Data on a person’s personality, intimacy, health condition, economic situation, opinions and beliefs; (2) Information that the Minister of Justice has determined by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, that it is sensitive information;

“Database manager” - An active manager of an entity that owns or holds a database or someone that such a manager has authorized for this matter;

“Registrar” - A person who meets the qualifications for appointment as a judge of a Magistrate’s Court, and whom the government has appointed, by notice in the Official Gazette, to manage the database registry (hereinafter - the Registry) as stated in section 12;

“Use," of information - (deleted);

“Data integrity” - The identity of the data in a database to the source from which it was drawn, without being changed, transmitted or destroyed without lawful permission.

In a criminal, civil or administrative trial for violation of privacy, it shall be a good defense if one of the following occurred:

The violation was done by way of publication that is protected under section 13 of the Prohibition of Defamation Law, 1965;

The defendant or the accused committed the violation in good faith under one of the following circumstances:

He did not know and should not have known about the possibility of violating privacy;

The violation was committed in circumstances where the violator had a legal, moral, social or professional duty to do so;

The violation was done to protect a legitimate personal interest of the violator;

The violation was committed while carrying out the violator’s lawful occupation and in the course of his regular work, provided it was not done by way of public publication;

The violation was by way of photography, or by way of publishing a photograph, taken in a public place and the image of the injured party appears in it incidentally;

The violation was done by way of publication that is protected under paragraphs (4) to (11) of section 15 of the Prohibition of Defamation Law, 1965;

There was public interest in the violation that justified it under the circumstances, provided that if the violation was by way of publication - the publication was not false.

### Definitions

23. In this chapter - “public body” -

Government ministries and other state institutions, local authority and other body fulfilling public functions by law;

A body that the Minister of Justice has determined by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, provided that the order specifies the types of information and knowledge that the body will be allowed to transmit and receive;

(Deleted)

“Database," “information," “Registrar” and “use” - (deleted).

### Cancellation

23a. The provisions of this chapter shall apply to information about a person’s private affairs, even if not within the definition of information, as they apply to information.

### Application to knowledge

23b. (a) The transfer of personal information from a public body is prohibited, unless the information has been published to the public by lawful authority, or has been made available for public inspection by lawful authority, or the person to whom the personal information relates has consented to the transfer.

(b) The provisions of this section do not prevent a security authority as defined in section 19 from receiving or transmitting personal information for the purpose of fulfilling its function, provided that the transmission or receipt has not been prohibited by law.

### Prohibition on information transfer

### 23c. Disclosure of personal information

Despite the provisions of section 23b, disclosure of personal information is permitted if not prohibited by law or principles of professional ethics:

Between public bodies, if one of the following is met:

The disclosure of personal information is within the powers or duties of the disclosing entity and is necessary for the purpose of implementing a law or for a purpose within the powers or duties of the disclosing or receiving entity;

The disclosure of personal information is to a public body authorized to demand such information by law from any other source;

From a public body to a government ministry or other state institution, or between such ministries or institutions, if the disclosure of personal information is necessary for the purpose of implementing any law or for a purpose within the powers or duties of the disclosing or receiving entity;

However, personal information given on condition that it not be disclosed to others shall not be disclosed as stated.

### Qualification to prohibition

23d. (a) A public body that regularly discloses personal information in accordance with section 23c shall specify this fact on every information request in accordance with the law.

(b) A public body that discloses personal information in accordance with section 23c shall maintain a record of the personal information disclosed.

(c) A public body that regularly receives personal information in accordance with section 23c, and the personal information is stored in a database, shall notify the Head of the Authority, and this fact shall be included in the details of the database registry list according to section 12.

(d) A public body that received personal information in accordance with section 23c shall not use it except within the scope of its powers or duties.

(e) Regarding the duty of confidentiality under any law, personal information disclosed to a public body by virtue of this law is equivalent to personal information that body obtained from any other source, and in addition, all provisions applicable to the disclosing body shall also apply to the receiving body.

### Obligations of a public body

### Excess personal information

23e. (a) Where personal information permitted to be disclosed under sections 23b or 23c is located on the same file with other personal information (hereinafter - excess personal information), the disclosing body may disclose to the receiving body the requested personal information along with the excess personal information.

(b) Disclosure of excess personal information under subsection (a) is contingent on establishing procedures that will ensure prevention of any use of the excess personal information received; such procedures shall be determined in regulations and until determined in regulations, the requesting body shall establish such procedures in writing, and provide the disclosing body with a copy thereof, upon request.

23f. Disclosure of personal information permitted under this law shall not constitute a violation of privacy and the provisions of sections 2 and 8 shall not apply to it.

### Permitted disclosure is not a violation of privacy

### Regulations regarding the transfer of personal information

23g. The Minister of Justice, with the approval of the Knesset Constitution, Law and Justice Committee, may enact regulations regarding procedures for transferring personal information from public bodies.

### Chapter D1: Supervisory Powers and Administrative Inquiry

### Section A: Appointment of Inspectors

23i. (a) The head of the Authority may appoint an inspector from among state employees, who will be granted the powers under this law, in whole or in part, if all of the following conditions are met:

The Israel Police has notified, within three months of the head of the Authority’s request, that it does not object to the appointment for reasons of public security, including due to criminal history;

He has received appropriate training in the area of powers to be granted to him under this law, and has met additional qualification conditions, if established, as directed by the Minister of Justice, with the consent of the Minister of National Security, and regarding the exercise of powers of intrusion into computer material or its copying as stated in section 23n - he holds a position skilled in performing such actions;

He has received appropriate training in the field of privacy protection, as directed by the Minister of Justice.

(b) The appointment of an inspector under this section shall be by a certificate signed by the head of the Authority, which attests to his role as an inspector and his powers under this law (hereinafter - inspector certificate).

(c) Notice of appointment under subsection (b) shall be published in the Official Gazette and on the website of the Privacy Protection Authority.

### Section B: Supervisory Powers

23j. (a) For the purpose of supervising the implementation of the provisions under Chapters B, D and E, and for the purpose of supervising the implementation of the provisions that the head of the Authority is authorized to order to cease their violation under section 23k, an inspector appointed under the provisions of Section A (hereinafter - an inspector) may -

Demand from any person he believes to be relevant to provide his name and address and present an identity card or other official document identifying him;

Demand from any relevant person to provide any information or document;

Demand from any relevant person to present to him or provide him with a copy of computer material including system data or sample information; Sample information under this section shall not be collected to an extent exceeding what is required for the realization of supervisory purposes;

Enter a place where he has reasonable grounds to believe that a database exists or is being used, provided that he does not enter a place used for residence except by court order.

### Translation

**(b)** Before exercising his powers under this section, the inspector shall inform the person that they are under inspection; once informed, the person must answer the questions asked, however, the answers given shall not be used as evidence in criminal proceedings against them, if they were not obligated to answer them had they been asked under section 2(2) of the Criminal Procedure Ordinance (Testimony).

**(c)** The head of the Authority shall delete system data or sample information provided or collected under subsection (a)(3) when they are no longer reasonably required for the continuation of inspection procedures, and at the latest within three years from the date of providing or collecting the information, and regarding system data - within seven years, unless the information is required for proceedings under Section B or C of this chapter, under Chapter D3 or under Chapter D4.

### Inspector’s Powers

23k. An inspector shall not use the powers granted to him under this chapter, except when performing his duty and when both of the following conditions are met:

He visibly wears a tag identifying him and his role;

He has an inspector’s certificate, which he will present upon request.

### Identification of Inspector

### Section C: Administrative Inquiry

23l. (a) If an inspector had reasonable grounds to believe that a violation of a provision that the head of the Authority is authorized to order its cessation under section 23kh or a provision under this law as stated in section 23kv has been committed, he may initiate an administrative inquiry procedure of the violation and exercise the powers in section 23j for this purpose.

(b) In an administrative inquiry procedure under subsection (a), the identification obligation under section 23k shall not apply if its fulfillment may cause one of the following:

Thwarting the execution of the inspector’s authority;

Harm to the security of the inspector or another person.

(c) Once the circumstance due to which an inspector did not fulfill the identification obligation as stated in subsection (b) has passed, the inspector shall fulfill his obligation as stated as soon as possible.

### Administrative Inquiry

23m. Before exercising his powers under this section, the inspector shall inform the person that an administrative inquiry procedure is being conducted regarding the database and the nature of the procedure; once informed, the person must answer the questions asked, however, the answers given shall not be used as evidence in criminal proceedings against them, if they were not obligated to answer them had they been asked under section 2(2) of the Criminal Procedure Ordinance (Testimony).

### Notice of Administrative Inquiry Procedure and Answering Inspector’s Questions

### Search and seizure warrant and warrant for penetration of computer material

23D. (a) If an inspector authorized by the head of the authority has reasonable grounds to believe that a violation of any of the provisions under this Law has been committed, as provided in section 23L(a), he may request from the court a search and seizure warrant or a warrant for penetration of computer material under sections 23(1), 23A and 24 of the Arrest and Search Ordinance, and carry them out himself or through another inspector; Notice of accreditation under this subsection shall be published in the Official Gazette.

(b) Information collected through penetration of computer material as part of an administrative investigation shall be used for the purpose for which it was collected only, and shall not be used as evidence in a criminal proceeding.

### How to search, seize an object and penetrate and copy computer material

23I. For searching, seizing an object and penetrating or copying computer material pursuant to this article, the provisions of sections 23A, 24(a)(1) and (b), 26 to 28, 31, 32A to 42 and 45 of the Arrest and Search Ordinance shall apply, with the following changes: The powers given to the police officer shall be vested in the inspector and the powers given to the officer shall be vested in the head of the authority or the inspector authorized to do so.

### Decision on an administrative inquiry procedure in case of reasonable grounds for suspicion of the existence of a criminal offense

23p. (a) If the head of the authority has reasonable grounds to suspect that an act or omission has been committed (in this chapter – an act) for which a criminal investigation may be conducted under Article A of Chapter D4 or an administrative investigation under this article, the head of the authority shall decide to conduct an investigation or administrative inquiry; The decision of the head of the authority as aforesaid shall be in accordance with these considerations only, and according to an enforcement procedure established by the head of the authority:

The severity and circumstances of the act;( 2) Assessing the nature and strength of the evidence related to that act;( 3) The enforcement policy of the Authority.

(b) If the head of the authority decides to conduct an administrative inquiry procedure as stated in subsection (a), and new facts have been discovered that were not previously known to the authority and which, had they been known to the authority, would have influenced the decision, the head of the authority may order an investigation to be conducted, instead of the clarification procedure.

(c) The head of the authority may delegate his authority under subsection (a), decide to conduct a criminal investigation or administrative investigation to a senior employee directly subordinate to him; Notice of such nobility shall be published in the Official Gazette.

### Article D: Lateral Supervision and External Experts

23g. (a) The head of the authority shall prescribe a plan for broad supervision of the implementation of provisions under this Law and a list of supervised entities to which the lateral supervision plan will apply; In order to implement the plan, the head of the authority may be assisted by a person who is not a civil servant in carrying out these activities (in this section – a facilitating party):

### Plan for Broad Supervision and Assistance from Non-Government Employees for Broad Supervision

Distribution of broad supervision questionnaires to supervised entities, provided it is clarified that the approach to the supervised entity is on behalf of the authority, but the response and dialogue will be conducted with a person who is not a government employee, and that the supervised entity will be entitled to contact the government employee whose name and contact details will be specified in the approach;

Receiving the response to the questionnaire from the supervised entity, along with the requested accompanying documents and additional documents attached by the supervised entity;

Examining the response to the questionnaire and documents received according to paragraph (2), according to criteria set by the head of the authority in procedures;

Contacting the supervised entity to receive completions or to update them on the need to clarify responses with the authority;

Preparing a report for the authority regarding the supervised entity’s response to the questionnaire for a specific supervised entity or type of supervised entities;

Granting extensions to supervised entities for responding to questionnaires or submitting documents according to the authority’s guidelines;

Answering technical questions from supervised entities.

**(b)** In performing the actions, the assisting entity will act in accordance with the instructions and directives of the head of the authority and under their supervision; however -

Any action requiring the exercise of discretion given to the authority or its employees by law will only be performed by a government employee;

An assisting entity will not perform an action that requires entry to a place in accordance with the provisions of section 23j(a)(4).

**(c)** The provisions of section 23r(c)(2) to (e), (g), (j) and (k) shall apply to an assisting entity, with the necessary changes.

### 23r.

For the purpose of supervising compliance with the provisions of Chapters B, D and E and for the exercise of his powers under Sections B and C and Chapter D3, the head of the authority may be assisted by a person who is not a government employee and who has an approval given to him according to the provisions of subsection (c) (in this law - external expert), in matters that require unique experience, knowledge or means.

An external expert will act on behalf of the head of the authority, in accordance with his instructions and directives and under his supervision; an external expert will not exercise authority involving the exercise of discretion given to the head of the authority or authority employees by law.

The head of the authority may give approval to serve as an external expert to someone who meets all of these:

He has experience, knowledge and expertise appropriate to his role;

He has not been convicted of an offense which, due to its nature, severity or circumstances, makes him unfit to serve as an external expert.

The head of the authority may not give approval to serve as an external expert to someone against whom criminal proceedings are pending for an offense which, due to its nature, severity or circumstances, makes him unfit to serve as an external expert.

**(e)**

No external expert shall be appointed or serve as an external expert as aforesaid, who, due to his tenure, will be frequently found in a situation of conflict of interest;

An external expert will not deal in the framework of his duties with an issue whose handling will cause him to be in a situation of conflict of interest;

If an external expert becomes aware that he may be in a situation of conflict of interest as stated in paragraphs (1) or (2), he shall notify the head of the authority as soon as possible.

**(f) An** external expert may require any person concerned to provide him with any information or document, provided that any requirement is approved in advance by an inspector, and he may also accompany an inspector entering the premises in accordance with the provisions of section 23J(a)(4).

**(g) An** external expert to whom information has been obtained pursuant to the provisions of this section while performing his duties or in the course of his work shall be kept secret, shall not disclose it to another and shall not make any use of it, except in accordance with the provisions of this Law or any other legislation or by order of a court.

### Assistance from an external expert

**(h)** A person who considers himself harmed by the action of an external expert may submit a reasoned complaint, in writing, to the head of the authority; The head of the authority will examine the complaint and respond to the applicant within 45 days; If the head of the authority finds that the complaint was justified, he shall notify the complainant and the external expert, together with his decision; If the head of the authority finds that the complaint was unjustified, he shall notify the complainant and the external expert in writing.

**(i)**

The law of an external expert as a civil servant with regard to the provisions relating to public servants in the Penal Law, 5737-1977, and the provisions in the Public Service (Gifts) Law, 5749-1979;

Limitations on the occupations of the external expert after the termination of the contract with him will be determined in the terms of the contract with him, including provisions regarding the period of time during which the external expert will not work for an entity that competes with the body that handled his case as an external expert and will not provide service to such body or receive a right or benefit from it.

**(j)** Notice of approval to serve as an external expert and the updated list of external experts will be published on the Authority's website.

**(k)** In this section—

"Family member" – spouse, parent, parent, son or daughter and their spouses, brother or sister and their children, mother-in-law, mother-in-law, grandson or granddaughter, including such relative who is intertwined (step);

"interested party" – as defined in the Securities Law, 5728-1968;

"Treatment" – including making a decision, raising a topic for discussion, attending a hearing, participating in a discussion or voting, or dealing with a topic outside of the discussion;

### Conflict of Interest and Oversight in Security Bodies

**“Conflict of interest”** of an external expert - a conflict between fulfilling their role and a personal interest or other position, of theirs or a relative;

**“Relative”** - any of the following:

A family member of an external expert;

A person whose financial situation the external expert has an interest in;

A corporation in which the external expert, their family member, or a person mentioned in paragraph (2) are stakeholders;

An entity in which the external expert, their family member, or a person mentioned in paragraph (2) are managers or responsible employees.

### Section E: Supervision and Administrative Inquiry in Bodies According to the Law for Regulating Security in Public Bodies

23t. The manner of exercising powers under Sections B and C regarding the bodies listed in the Fifth Addendum to the Law for Regulating Security in Public Bodies shall be determined in a procedure formulated in agreement between the National Cyber Array as defined in the said law (in this law - the National Cyber Array) and the Authority, taking into account the sensitivity of information and computerized systems used by these bodies.

### Chapter D2: Supervision and Administrative Inquiry in Security Bodies

23k. (a) In this chapter -

**“Security body”** means one of the following:

Israel Police;

Israel Defense Forces;

General Security Service;

The Institute for Intelligence and Special Operations;

The National Cyber Array;

The Witness Protection Authority;

Israel Prison Service;

Ministry of Defense and its subordinate units and the Security Officer in the Defense Establishment;

Units and subordinate units of the Prime Minister’s Office, whose main activity is in the field of state security;

Enterprises included in an order issued by the Minister of Defense under item (3) in the First Addendum to the Law for Regulating Security in Public Bodies, which the Minister of Defense has notified to the Minister of Justice;

Another body determined by the Minister of Defense, by order, with the consent of the Minister of Justice and with the approval of a joint committee of the Constitution Committee and the Foreign Affairs and Defense Committee of the Knesset;

**“Head of a security body,"** regarding the Israel Defense Forces - the Chief of General Staff or an officer with the rank of Major General whom the Chief of General Staff has authorized for this matter.

(b) (1) The provisions of Sections B and C in Chapter D1 shall not apply to security bodies, but supervision and administrative inquiry in security bodies shall be carried out according to the provisions of this chapter;

### Applicability to Security Bodies

(c) The Minister of Defense, with the consent of the Minister of Justice, may choose not to include in the official publication of an order as mentioned in paragraph (11) of the definition of “security body” in subsection (a), the name of the body for which the said order was issued, for reasons of maintaining state security; however, the full text of the order, including the name of the said body, shall be deposited with the Minister of Justice.

### Applicability to Security Bodies

From 14-08-2028

23k. (a) In this chapter –

“Security body” means one of the following:

Israel Police;

Israel Defense Forces;

General Security Service;

The Institute for Intelligence and Special Operations;

National Cyber Array;

Witness Protection Authority;

Israel Prison Service;

Ministry of Defense and its subsidiary units and the Security Officer in the Defense Establishment;

Units and subsidiary units of the Prime Minister’s Office, whose main activity is in the field of state security;

Enterprises included in an order issued by the Minister of Defense according to item (3) in the First Schedule to the Law for Regulating Security in Public Bodies, and which the Minister of Defense has notified to the Minister of Justice;

### Applicability to Security Bodies

Another body determined by the Minister of Defense, by order, with the consent of the Minister of Justice and with the approval of a joint committee of the Constitution Committee and the Foreign Affairs and Defense Committee of the Knesset;

“Head of a security body," regarding the Israel Defense Forces – the Chief of the General Staff or an officer with the rank of Major General whom the Chief of the General Staff has authorized for this matter.

(b) (1) The provisions of Sections B and C in Chapter D1 shall not apply to security bodies, however, supervision and administrative inquiry in security bodies shall be carried out according to the provisions of this chapter;

Notwithstanding the provisions of paragraph (1), the provisions of Sections B and C of Chapter D1 shall apply to the Israel Police, provided that they do not apply to databases classified as “Secret” and above.

(c) The Minister of Defense, with the consent of the Minister of Justice, may choose not to include in the official publication of an order as mentioned in paragraph (11) of the definition of “security body” in subsection (a), the name of the body for which the said order was issued, for reasons of maintaining state security; however, the full text of the order, including the name of the said body, shall be deposited with the Minister of Justice.

23ka. (a) The head of a security body, in consultation with the head of the Authority, shall appoint a person to the position of privacy inspector in the security body (in this chapter – the internal inspector), in accordance with qualification and training conditions to be directed by the head of the Authority, in consultation with the head of the security body.

**Translation:**

(b) The internal inspector shall be appointed for one term of office, and the head of the security body may appoint them for additional terms of office, in consultation with the head of the Authority; the term of office of the internal inspector shall not be less than three years.

(c) The term of office of the internal inspector shall not be terminated and they shall not be removed from their position except in consultation with the head of the Authority.

(d) The internal inspector shall be an employee of the security body directly subordinate to the head of the security body, or to a senior employee in the security body directly subordinate to the head of the security body, and they shall be professionally guided by the head of the Authority.

(e) The internal inspector shall not fulfill an additional role and shall not engage in an additional occupation that may place them in a conflict of interest in fulfilling their role under this chapter.

(f) The security body shall provide the internal inspector with adequate means necessary to fulfill their role under this chapter.

### Appointment of a Privacy Inspector in a Security Body

23b. The internal inspector shall supervise the implementation of the provisions of this law in the security body and shall maintain control over their execution, including:

Prepare an annual work plan to be submitted for approval to the head of the security body and the head of the Authority, for supervising the compliance with the provisions of this law and for examining violations of provisions that the head of the Authority is authorized to order their cessation according to section 23e and violation of a provision of the provisions under this law listed in section 23f (in this section - work plan);

Examine the procedures of the security body and its policy in the field of privacy protection and their compliance with the provisions of the law and the security body’s policy in the field of privacy protection and its compliance with the provisions under this law;

Examine the existence of violations of provisions that the head of the Authority is authorized to order their cessation according to section 23e and violation of provisions under this law listed in section 23f, in accordance with the instructions of the head of the Authority;

Report to the head of the Authority without delay, subject to the provisions of security clearance, as defined in section 15 of the General Security Service Law, 2002, and the compartmentalization applicable to the security body, on findings of supervision and inspection activities performed;

Maintain control over the manner of correcting deficiencies discovered in the findings of supervision and inspection;

Conduct training and instruction of employees of the security body on privacy issues;

### Duties of the Internal Inspector

Submit to the head of the security body and the head of the Authority an annual report on the manner of execution of the work plan and on compliance with the provisions of the law in the field of privacy in the security body.

23c. For the purpose of fulfilling their role, the internal inspector shall have the powers granted to an inspector under Chapter D1, Section B, and shall also be subject to the obligation to delete sample information as stated in section 23j(c), with the necessary changes.

### Powers of the Internal Inspector

**23d. (a)** The head of the Authority may instruct the internal inspector to carry out actions, including complementary actions or additional actions beyond those performed by the internal inspector, or to act to correct deficiencies.

**(b)** The head of the Authority may use the powers vested in him under Chapter D3 if he found that a provision from the provisions that the head of the Authority is authorized to order the cessation of their violation under section 23e or a provision listed in section 23f has been violated, based on a report by the internal inspector, or if he found that there is concern that a provision from the provisions listed as mentioned has been violated and instructed the internal inspector to investigate whether a violation was committed, and the internal inspector did not investigate the violation within a reasonable time set by the head of the Authority after consulting with the internal inspector, and the provisions of section 23g were fulfilled.

**(c)** If the head of the Authority believes that the findings as stated in subsection (a) or (b) raise suspicion of committing an offense under this law or if he became aware in another way of the commission of such an offense, the investigator will have enforcement powers under section 23na, unless there was another investigative authority competent by law to investigate offenses in that security body; For the purpose of this section, “another investigative authority” - except for the Israel Police.

**(d)** An investigator or the head of the Authority shall not use his powers under this chapter towards a security body, except after undergoing security clearance as defined in section 15 of the General Security Service Law, 2002.

### Powers of the Head of the Authority Regarding Security Bodies

### Chapter D3: Administrative Enforcement Measures and Judicial Order

### Section A: Authority of the Head of the Authority to Order Cessation of Violation

**23e. (a)** If the head of the Authority found that a controller of a database or a holder of a database used information about a person’s private affairs in a database for a purpose other than that for which it was provided, contrary to the provisions of section 2(9), or processed personal information in a database for a purpose that constitutes a violation of privacy under section 2, he may, after giving him an opportunity to present his arguments, notify him that his actions constitute a violation and order him to cease it in the manner and within the period he will instruct.

**(b)** If the head of the Authority found that a controller of a database or a holder of a database processed personal information in a database that was created, received, accumulated or collected, contrary to the provisions of this law or contrary to the provisions of any other law regulating information processing, or allowed another to process personal information as mentioned on his behalf, contrary to section 8(d), he may, after giving him an opportunity to present his arguments, notify him that his actions constitute a violation and order him to cease it in the manner and within the period he will instruct.

### Authority to Order Cessation of Violation

(c) If the head of the Authority finds that a controller or processor of a database processed information in violation of the regulations listed in Part B of the Fourth Schedule, he may, after giving them an opportunity to present their arguments, notify them that their actions constitute a violation and order them to cease it in the manner and within the period he directs.

(d) If the head of the Authority finds that the provisions of paragraphs (1) to (4) below have been met, he may, after giving the controller or processor of the database required to appoint a privacy protection officer under section 17b(1a) an opportunity to present their arguments, notify them that their actions constitute a violation, and order them to cease the violation and the manner in which they must correct it; if the Minister of Justice, with the approval of the Constitution Committee, issued an order under section 23kv(d)(1)(g), the head of the Authority may also issue such an order regarding paragraph (5) below:

The privacy protection officer was not provided with the conditions and resources necessary for the proper fulfillment of their role or was not properly involved in all matters relating to privacy protection laws, contrary to section 17b(2b);

The privacy protection officer does not report directly to the position holders listed in section 17b(2c);

The privacy protection officer does not possess the knowledge and qualifications required under section 17b(3a);

The privacy protection officer holds an additional position or is subordinate to an officer in the body where they perform their role or in another body in a manner that may put them at risk of conflict of interest in fulfilling their duties under this law, contrary to section 17b(3c);

The controller or processor of the database did not appoint a privacy protection officer, contrary to section 17b(1a)(3) or (4).

(e) In an order to cease violation under subsections (a) to (d), the head of the Authority shall specify the following:

Details of the act or omission (in this chapter - the act) constituting the violation, the circumstances of its commission and the date of its commission, the requirement to correct the violation and the deadline for its correction;

The possibility that a monetary sanction will be imposed on the violator if they do not cease the violation;

The violator’s right to file an appeal within 45 days under subsection (f).

(f) (1) An order by the head of the Authority to cease a violation may be appealed to the Magistrate’s Court where the President of the Magistrate’s Court sits, within 45 days from the day the notice of cessation of violation was delivered;

(2) The court hearing the appeal may confirm the decision of the head of the Authority, modify it, cancel it or make another decision in its place, and may return the matter with instructions to the head of the Authority;

If an appeal is filed as stated, a violation of the head of the Authority’s instruction under this section will not be considered a violation until the court orders otherwise.

(g) The head of the Authority may delegate his powers under subsections (a) to (c) to a senior employee directly subordinate to him; notice of such delegation shall be published in the Official Gazette.

### Chapter B: Imposition of Monetary Sanctions

23f. (a) If a controller of a database or a processor of a database violates any of the provisions of this law, as detailed below, the head of the Authority may impose on him a monetary sanction in the amount of 150,000 New Shekels, and if the database contained personal information about 1,000,000 people or more, the head of the Authority may impose double the amount:

Did one of the following:

Processed personal information in a database required to be registered without being registered, in violation of the provisions of section 8a(a);

Included incorrect details in an application for registration of a database submitted under section 9, in violation of the provisions of that section;

Did not notify the head of the Authority of a change in the details listed in section 9(b) or in details determined under section 9(c), in violation of the provisions of section 9(d), except for a change in the address of the controller of the database;

Did not submit to the head of the Authority a notice about a database required to be notified under section 8a(b) or did not notify the head of the Authority of a change in any of the details specified in that section, in violation of the provisions of that section;

Processed personal information in a database used for direct mailing services, without the database being registered in the registry or without one of the registered purposes of the database being direct mailing services, in violation of the provisions of section 17d;

Did not notify the head of the Authority that he regularly receives personal information in accordance with the provisions of section 23c and the information is stored in a database, in violation of the provisions of section 23d(c).

(b) If a controller of a database or a processor of a database violates any of the provisions of this law, as detailed below, the head of the Authority may impose on him a monetary sanction according to the provisions of this chapter, in the amount of 15,000 New Shekels:

Refused to allow a person whose personal information is held in the database to review the personal information about him, in violation of the provisions under section 13;

Made a change to the personal information in his possession without notifying everyone who received the information, in violation of the provisions under section 14(b);

Did not notify the requester of a refusal to correct personal information in a database he owns or to delete it, in violation of the provisions under section 14(c);

Did not correct personal information in a database in his possession, in violation of the provisions of section

Did not comply with a person’s request in accordance with Section 17f(b) to delete personal information relating to them from a database used for direct mailing, in violation of the provisions of Section 17f(d); (6) Did not comply with a person’s request in accordance with Section 17f(c) that personal information relating to them should not be disclosed to a person, type of persons, or specific individuals, in violation of the provisions of Section 17f(d). (c) (1) If a database controller or database holder violated any of the provisions under this law, as detailed below, the Head of the Authority may impose a financial sanction according to the provisions of this chapter, in an amount equal to the multiplication of 50 New Israeli Shekels by the number of individuals to whom the request or demand was made, as detailed below, and if the request or demand was regarding information of special sensitivity - in an amount equal to the multiplication of 100 New Israeli Shekels by the number of such individuals: (a) Approached a person to obtain personal information for processing in a database, without providing the required notice under Section 11; (b) Approached a person through direct mailing, in violation of the provisions of Section 17f(a); (c) A database controller who did not specify on a request for personal information that they regularly provide information in accordance with Section 23c, in violation of the provisions of Section 23d(a); (2) If the amount of the financial sanction under paragraph (1) was less than 30,000 New Israeli Shekels, the Head of the Authority may impose on a database controller or database holder a financial sanction in the amount of 30,000 New Israeli Shekels. (d) (1) If a database controller or database holder violated any of the provisions under this law, as detailed below, the Head of the Authority may impose a financial sanction according to the provisions of this chapter in the amount of 2 New Israeli Shekels for each person whose personal information is in the database, and if the personal information in the database was information of special sensitivity - in the amount of 4 New Israeli Shekels for each person: (a) Approached a person to obtain personal information for processing in a database, and the approach was made to an unspecified group of people, without providing the required notice under Section 11, in violation of the provisions of said section; (b) Did not appoint an information security officer, in violation of the provisions of Section 17b(a); (c) Did not appoint a privacy protection officer, in violation of the provisions of Section 17b(1a)(1) or (2); (d) Processed personal information in a database used for direct mailing services, without having a record indicating the source from which each dataset used for the database was received and the date of its receipt, as well as a record indicating to whom each such dataset was provided, in violation of the provisions of Section 17e;

(ה) A database controller who did not maintain a record of personal information provided in accordance with section 23c, in violation of section 23d(b);

(ו) Regarding a database controller listed in section 17b(1a)(1) or (2) - did not comply with the Authority head’s instructions to cease or correct a violation, in violation of section 23kh(d);

(ז) The Minister of Justice, with approval of the Constitution Committee, may order that the provisions of sub-paragraph (ו) also apply to a database controller or holder listed in section 17b(1a)(3) and (4);

(2) For monetary sanctions under sub-paragraphs (ד) and (ה), the amount shall be calculated based on the number of individuals for whom there is no record as stated in those sub-paragraphs;

(3) If the monetary sanction amount under paragraph (1) is less than 20,000 new shekels, or if the personal information in the database was particularly sensitive information - less than 40,000 new shekels, the Authority head may impose on the database controller or holder a monetary sanction of 20,000 new shekels or 40,000 new shekels, as applicable.

(ה)(1) If a database controller or holder violated any of the following provisions of this law, the Authority head may impose a monetary sanction under this chapter in the amount of 4 new shekels for each person whose personal information is in the database, and if the personal information in the database was particularly sensitive information - in the amount of 8 new shekels for each person:

Did not comply with the Authority head’s instructions under section 23kh(a) to cease using information about a person’s private affairs in a database for a purpose other than that for which it was provided, in violation of section 2(9), or to cease processing personal information in a database for a purpose that constitutes a violation of privacy under section 2;

Processed personal information in a database for an unlawful purpose, in violation of section 8(b), unless the processing was only in violation of section 2;

Did not comply with the Authority head’s instructions under section 23kh(b) to cease processing personal information in a database that was created, received, accumulated or collected in violation of this law or any other law regulating information processing, or to cease allowing another to process such personal information on its behalf;

Processed personal information without authorization from the database controller, or exceeding such authorization, in violation of section 8(c);

A database controller who provided information from a public body, in violation of section 23b, without meeting the requirements of section 23c;

If the amount of the monetary sanction as stated in paragraph (1) is less than 200,000 New Israeli Shekels, the head of the Authority may impose on a database controller or database holder a monetary sanction in the amount of 200,000 New Israeli Shekels.

**(f)** If a database controller or database holder processed personal information in a database not in accordance with the purpose specified for it, in violation of the provisions of section 8(b), in circumstances where such a purpose could have been legally determined, the head of the Authority may impose on them a monetary sanction according to the provisions of this chapter in the amount specified in item (1) of the Third Schedule.

**(g)** If a database controller or database holder did not provide a document or copy of computer material to an inspector, in violation of the provisions of section 23j(a)(2) or (3), the head of the Authority may impose on them a monetary sanction according to the provisions of this chapter in the amount of 300,000 New Israeli Shekels.

**(h)** If a database controller or database holder violated any of the provisions of the regulations established under section 36, as detailed in column A of the Third Schedule, applicable to them, the head of the Authority may impose on them a monetary sanction according to the provisions of this chapter in the amount specified in column B, C, D or E next to that provision, as applicable. If the database is subject to the highest level of security in the said Schedule and contains information about 1,000,000 people or more, the head of the Authority may impose double the amount specified in column E next to that provision.

(1) If a database controller or database holder violated any of the provisions of the regulations established under section 36, in the Fourth Schedule, as detailed in column A of Part A of that Schedule, the head of the Authority may impose on them a monetary sanction according to the provisions of this chapter in the amount specified in column B next to that provision;

(2) If a database controller or database holder did not comply with the instructions of the head of the Authority under section 23k(c) to cease the violation of the regulations’ provisions as stated in Part B of the Fourth Schedule, the head of the Authority may impose on them a monetary sanction according to the provisions of this chapter, in the amount specified in column B next to that provision in that Schedule.

**(j)** (1) If a payment demand was delivered to a database holder due to a violation of a provision as stated in subsection (h), the head of the Authority shall notify the database controller of this, attaching a copy of the payment demand delivered to the holder, and shall instruct the database controller to act to cease the violation by the holder, all within a period as the head of the Authority shall instruct;

(2) If the violation as stated in paragraph (1) was not ceased and the database controller did not perform what the head of the Authority demanded of them for the purpose of ceasing the violation, the head of the Authority may

To deliver a notice of intent to charge as stated in section 23-27 for that violation, and the provisions under this section shall apply to the controlling owner of the information database regarding that violation, with necessary changes, as if he were the violator; the amount of the monetary sanction to be imposed on the controlling owner of the information database for such a violation shall be the amount that can be imposed on the holder for the same violation.

### Notice of intent to charge

23-27. (a) If the head of the Authority has reasonable grounds to believe that a person has violated a provision of the provisions under this law, as stated in section 23-26 (in this chapter - the violator), and intends to impose a monetary sanction on him according to that section, he shall deliver to the violator a written notice of the intention to impose a monetary sanction on him (in this law - notice of intent to charge).

(b) In the notice of intent to charge, the head of the Authority shall specify, among other things, the following:

Details of the act constituting the violation, the circumstances of its commission and the date of its commission;

The amount of the monetary sanction and the period for its payment;

The right of the violator to present his arguments before the head of the Authority according to the provisions of section 23-28, and that the notice of intent to charge will be considered as a payment demand if the violator does not exercise the said right, as stated in section 23-29(d);

The authority to add to the amount of the monetary sanction for a continuing violation or repeated violation according to the provisions of section 23-30, and the rate of addition.

### Right of hearing

23-28. A violator who has been given a notice of intent to charge according to the provisions of section 23-27 may present his arguments, before the head of the Authority, in writing or orally, according to the decision of the head of the Authority, regarding the intention to impose a monetary sanction on him and regarding its amount, within 45 days from the date of delivery of the notice; the head of the Authority may extend the said period, for special reasons that will be recorded.

### Decision of the head of the Authority and payment demand

23-29. (a) The head of the Authority shall decide, after considering the arguments presented according to section 23-28, whether to impose a monetary sanction on the violator, and may reduce the amount of the monetary sanction according to the provisions of section 23-31.

(b) If the head of the Authority decides according to subsection (a) -

To impose a monetary sanction on the violator - he shall deliver to him a demand, in writing, to pay the monetary sanction (in this chapter - payment demand), in which he shall specify, among other things, the updated amount of the monetary sanction and the period for its payment, as well as the right of the violator to file an appeal within 45 days according to section 23-45;

Not to impose a monetary sanction on the violator - he shall deliver to him a notice of this, in writing.

(c) In the payment demand or notice, according to subsection (b), the head of the Authority shall detail the reasons for his decision.

(d) If the violator did not present their arguments according to the provisions of section 23(28) within the period specified in that section, the notice of intent to charge shall be considered, at the end of that period, as a payment demand delivered to the violator at the said time.

23(30). (a) (1) In a continuing violation, one-hundredth of the fixed monetary sanction for that violation shall be added for each day the violation continues; for this purpose, “continuing violation” means violation of a provision under this law, as stated in section 23(26), after a payment demand was delivered to the violator for violating that provision;

(2) If an appeal was filed against the payment demand decision, the period until the court’s ruling on the matter shall not be counted for the purpose of paragraph (1), unless the court decides otherwise.

(b) In a repeated violation, an amount equal to the monetary sanction shall be added to the fixed monetary sanction for that violation; for this purpose, “repeated violation” means violation of a provision under this law, as stated in section 23(26), committed after the date for payment of the monetary sanction, within two years of a previous violation of the same provision for which a monetary sanction was imposed on the violator or for which they were convicted.

### Continuing Violation and Repeated Violation

23(31). The head of the Authority is not authorized to impose a monetary sanction in an amount lower than the amounts set according to this chapter, except in cases, circumstances, and according to considerations detailed in the Fifth Schedule and at the rates specified therein.

### Reduced Amounts

23(32). (a) The monetary sanction shall be according to its updated amount on the day of delivery of the payment demand, and regarding a violator who did not present their arguments before the head of the Authority as stated in section 23(29)(d) - on the day of delivery of the notice of intent to charge; if an appeal was filed with the court and the payment of the monetary sanction was delayed by the head of the Authority or by the court - the monetary sanction shall be according to its updated amount on the day of the decision on the appeal, as applicable.

(b) The amounts set in section 23(26) and the amounts set in the Third Schedule, Fourth Schedule, and Fifth Schedule shall be updated on January 1st of each year (in this subsection - the update day), according to the rate of change of the known index on the update day compared to the index that was known on January 1st of the previous year; the said amount shall be rounded to the nearest amount that is a multiple of 10 new shekels; the first update according to this subsection shall be in 2026; for this purpose, “index” means the Consumer Price Index published by the Central Bureau of Statistics.

(c) The head of the Authority shall publish in the Official Gazette and on the Authority’s website a notice of the updated amounts of the monetary sanction according to subsection (b).

### Updated Amount of the Monetary Sanction

23לג. The date of payment of the monetary sanction

The violator must pay the monetary sanction within 45 days from the day the payment demand is delivered as stated in section 23כט.

23לד. Shekel interest and late payment fees

If the monetary sanction is not paid on time, shekel interest and late payment fees will be added for the period of delay, until payment, and the provisions of the Interest and Linkage Ruling Law, 1961, will apply with the necessary changes.

23לה. Collection

A monetary sanction will be collected for the State Treasury, and the Collection Center for Fines, Fees and Expenses Law, 1995, will apply to its collection.

### Section C: Administrative Warning

23לו. Administrative warning

If the head of the Authority had reasonable grounds to believe that a person violated one of the provisions under this law, as stated in section 23כו, and circumstances determined by the Minister of Justice existed, the head of the Authority may, instead of imposing a monetary sanction according to the provisions of Section B, deliver an administrative warning according to the provisions of this section.

In an administrative warning, the head of the Authority will specify the act constituting the violation, the circumstances of its commission and the date of its commission, inform the violator that they must cease the violation and that if they continue or repeat the violation they will be subject to a monetary sanction for a continuing or repeated violation, as applicable, and the method of calculating the sanction amount, as stated in section 23לח, and will also indicate the violator’s right to request cancellation of the warning according to the provisions of section 23לז.

23לז. Request to cancel administrative warning

If an administrative warning was delivered to a violator as stated in section 23לו, they may approach the head of the Authority, in writing, within 45 days, with a request to cancel the warning for any of these reasons:

The violator did not commit the violation;

The act committed by the violator, detailed in the warning, does not constitute a violation.

The head of the Authority may extend the period stated in subsection (a), for special reasons that will be recorded.

If the head of the Authority received a request to cancel an administrative warning, according to the provisions of subsection (a), they may cancel the warning or reject the request and leave the warning in place; the head of the Authority’s decision will be given in writing and delivered to the violator with reasons.

23לח. Continuing violation after administrative warning

If an administrative warning was delivered to a violator according to the provisions of this section and the violator continued to violate the provision for which the warning was delivered, the violation will be considered a continuing violation, and the provisions of section 23ל(a) will apply, and the head of the Authority will deliver to the violator a notice of intent to charge for the continuing violation in accordance with the provisions of section 23כז, with the necessary changes.

**Continuous Violation and Repeated Violation After Warning**

### Section D: Commitment to Avoid Violation

23.39. Notice of Possibility to Submit Commitment and DepositIf the head of the Authority has reasonable grounds to believe that a person has violated a provision of the provisions under this law, as stated in section 23.26, and circumstances determined by the Minister of Justice exist, the head of the Authority may deliver to the violator a written notice about the possibility to submit a letter of commitment to the head of the Authority and deposit a guarantee according to the provisions of this section, instead of the monetary sanction that can be imposed on him according to the provisions of section B.

23.40. Terms of Commitment and Amount of Deposit(a) In the letter of commitment, the violator shall commit to cease the violation of the provision as stated in section 23.39 and to refrain from further violation of the same provision, within a period determined by the head of the Authority starting from the day of submitting the letter of commitment, provided that the said period does not exceed two years (in this section - the commitment period).

(b) The head of the Authority may set additional conditions in the letter of commitment that the violator must commit to and comply with during the commitment period, in order to reduce the damage caused by the violation or prevent its recurrence.

(c) In addition to the letter of commitment, the violator shall deposit with the Authority a guarantee in the amount of the monetary sanction that the head of the Authority would have been entitled to impose on the violator for that violation, taking into account the existence of circumstances and considerations listed in the Fifth Schedule.

(d) The head of the Authority may, at the request of the violator and for reasons to be recorded, exempt the violator from depositing the guarantee under subsection (c) or reduce the amount of the guarantee that the violator will deposit under that subsection.

23.41. Consequences of Submitting a Letter of Commitment and Deposit or Non-Submission(a) If the violator submitted to the head of the Authority a letter of commitment and deposited a guarantee according to this section, within 45 days from the day of delivery of the notice as stated in section 23.39, no monetary sanction will be imposed on him for that violation; if the violator did not submit to the head of the Authority a letter of commitment or did not deposit a guarantee within the said period, the head of the Authority will deliver to him a notice of intent to charge for that violation, according to section 23.27.

(b) The head of the Authority may extend the period stated in subsection (a), for special reasons to be recorded.

### Breach of Commitment

**23M. (a)** If the violator submitted a letter of commitment and deposited a guarantee according to this section and violated one of the conditions of the commitment, as detailed in the following paragraphs, the provisions detailed in those paragraphs shall apply, as appropriate:

If the violator, during the commitment period, continued to violate the provision for which he gave the letter of commitment, or repeatedly violated the said provision during that period, such violation shall be considered as a continuous violation for the purpose of section 23L(a) or as a repeated violation for the purpose of section 23L(b), as applicable, and the following provisions shall apply:

The head of the authority shall deliver to the violator a notice of intent to charge for the continuous violation or the repeated violation, as applicable, in accordance with the provisions of section 23K, with the necessary changes;

If the head of the authority delivered to the violator a payment demand for the continuous violation or the repeated violation, as applicable, in accordance with the provisions of section 23N(b)(1), or if the violator did not present his arguments before the head of the authority regarding that violation as stated in section 23N(d), the head of the authority shall forfeit the guarantee in addition to imposing the monetary sanction for the continuous violation or the repeated violation; If the head of the authority decided, according to section 23M(d), to exempt the violator from depositing the guarantee or to reduce the amount of the guarantee, he shall deliver to the violator a payment demand according to section 23N which also includes the amount of the guarantee for which the exemption was given or the part that was reduced from the guarantee amount, as applicable, plus shekel interest, from the day of the head of the authority’s decision on the exemption or reduction as stated until the day of delivery of the payment demand;

If the violator violated one of the additional conditions set in the letter of commitment as stated in section 23M(b) - the head of the authority shall forfeit the guarantee, and if he decided, according to section 23M(d), to exempt the violator from depositing the guarantee or to reduce the amount of the guarantee, he shall deliver to the violator a payment demand according to section 23N regarding the amount of the guarantee for which the exemption was given or regarding the part that was reduced from the guarantee amount, as applicable, plus shekel interest from the day of the head of the authority’s decision on the exemption or reduction as stated until the day of delivery of the payment demand; The head of the authority shall not forfeit the guarantee or send a payment demand according to this paragraph unless he has given the violator an opportunity to present his arguments, in writing, regarding the violation of the conditions as stated.

**(b)** For the purpose of this chapter, the forfeiture of the guarantee according to the provisions of this section shall be considered as imposing a monetary sanction on the violator for the violation for which the guarantee was given.

### (c) Violation of Commitment Terms

If a condition of the commitment as stated in this section is violated, and the violator breaches again the provision for which they gave the letter of commitment, the head of the authority will not allow them to submit an additional letter of commitment according to the provisions of this section, for the same violation.

### 23m. Return of Deposit

If the violator complies with the terms of the letter of commitment submitted according to this section, the deposit they made will be returned to them at the end of the commitment period, with shekel interest from the day of deposit until the day of return.

### Section E: Miscellaneous Provisions Regarding Financial Sanctions

### 23md. Financial Sanction for Violation of Multiple Provisions

For a single act that constitutes a violation of several provisions under this law, as well as an act that constitutes a violation of a provision listed in section 23k and a violation under another law, no more than one financial sanction shall be imposed.

### 23me. Appeal, Stay of Execution, and Refund

The implementation of administrative enforcement measures according to sections B to E can be appealed to the Magistrate’s Court where the President of the Magistrate’s Court sits, within 45 days from the day the notice of the action was delivered.

The submission of an appeal on the decision of the head of the authority according to sections B to E does not delay the execution of the decision, unless the head of the authority agreed to it or the court ordered so.

The court hearing the appeal may approve the decision of the head of the authority, change it, cancel it, or make another decision in its place, and it may return the matter with instructions to the head of the authority.

If the court decided, after the financial sanction was paid or the deposit was made, to accept an appeal as stated in subsection (a), and ordered the return of the paid financial sanction amount or the reduction of the financial sanction or the return of the deposit, the amount paid or any reduced part of it or the deposit will be returned, as applicable, with shekel interest from the day of payment or deposit until the day of return.

### 23mf. Publication

If the head of the authority imposed a financial sanction according to this chapter, they will publish the following details on the website of the Privacy Protection Authority, in a way that ensures transparency regarding the exercise of discretion in the decision to impose a financial sanction:

The fact of imposing the financial sanction;

The nature of the violation for which the financial sanction was imposed, the date of the violation, and the circumstances of the violation;

The amount of the financial sanction imposed;

If the financial sanction was reduced - the circumstances due to which the amount of the financial sanction was reduced and the rates of reduction;

Details about the violator, relevant to the matter;

The name of the violator - if it is a corporation, unless it is a corporation managed by an individual and the name of the corporation is the same as the name of its sole owner.

Publication under this section shall not be carried out until the violator has been given an opportunity to present their arguments; the opportunity to present arguments under this subsection may be given to the violator as part of the right to a hearing under section 23(28), provided that the head of the Authority notifies the violator of the intention to publish their name in the notice of intent to charge under section 23(27).

If an appeal is filed against the decision of the head of the Authority to impose a monetary sanction, the head of the Authority shall publish, in the same manner as published under subsection (a), the fact of the filing of the appeal and its results.

Notwithstanding the provisions of subsection (a)(6), the head of the Authority -

Shall not publish the name of a violator that is a corporation, if convinced that the violation is minor under the circumstances, unless publication is necessary to warn the public whose details are in the database;

Shall publish the name of an individual violator or a corporation whose name is the same as its sole owner, if deemed necessary to warn the public.

Notwithstanding the provisions of this section, the head of the Authority shall not publish details that constitute information that a public authority is prohibited from disclosing under section 9(a) of the Freedom of Information Law, and may also refrain from publishing details under this section that constitute information that a public authority is not obligated to disclose under section 9(b) of the said law.

Publication under this section regarding a monetary sanction imposed on a corporation shall be for a period of four years, and regarding a monetary sanction imposed on an individual - for a period of two years.

The Minister of Justice, with the approval of the Constitution Committee, may determine additional ways to publish the details mentioned in this section.

### Publication

**23(47). (a)** Payment of a monetary sanction, issuance of an administrative warning, or submission of a letter of commitment and deposit of a guarantee, under this chapter, shall not detract from a person’s criminal liability for violating any of the provisions under this law that constitutes an offense.

**(b)** Notwithstanding the provisions of subsection (a), if a violator has been given notice of intent to charge, an administrative warning, or notice of the possibility to submit a letter of commitment and deposit a guarantee, for a violation that also constitutes an offense, an indictment shall not be filed against them for that violation, unless new facts are discovered that justify it, as stated in section 23(16); if new facts are discovered as stated and an indictment is filed against the violator after the violator has paid a monetary sanction or deposited a guarantee, the amount paid or the guarantee deposited, as applicable, shall be returned to them, with the addition of shekel interest and late payment fees from the day of payment of the amount or from the day of deposit of the guarantee, until the day of its return.

### Preservation of Criminal Liability

**(c)** If an indictment is filed against a person for an offense that constitutes a violation, the head of the Authority shall not take proceedings against them under sections B to E for the violation.

### Delegation of Authority

23M. The head of the Authority may delegate their powers under sections B to E to a senior employee directly subordinate to them and responsible for the area of monetary sanctions; notice of such delegation shall be published in the Official Gazette.

### Section F: Judicial Cessation Order

23N. (a) If the head of the Authority has reasonable grounds to believe that a violation of the provisions under section 2(9), 8(b), (c) or (d), 17 or 23b is being or about to be committed in a database, they may request the Administrative Affairs Court (in this section - the Court) to issue an order to the database controller or processor to cease data processing operations causing or likely to cause the violation (in this section - cessation order), and the Court may also order the complete deletion of personal data in the database (in this section - deletion order).

(b) The Court may issue an order under subsection (a), as requested or with modifications, if convinced that all of the following are met:

There are reasonable grounds to believe that a violation as stated in that subsection is being or about to be committed in a database;

There is no less harmful means to prevent the violation;

The potential damage from the violation exceeds the potential damage from issuing the order, including potential harm to freedom of expression;

The severity of the violation justifies issuing the order.

(c) (1) An order under this section shall be issued after giving the database controller an opportunity to present their arguments before the Court, and if the order is directed at a processor - also to the processor, as far as possible and in a manner appropriate to the circumstances;

A cessation order without the presence of a party as stated in paragraph (1) shall be issued for a period not exceeding 48 hours; during such period, a deletion order shall not be issued;

The Court may extend the validity of the order after giving the database controller or processor, as applicable, an opportunity to present their arguments.

(d) The Court may reconsider an order under this section if it sees justification due to changed circumstances or new facts discovered after issuing the order.

(e) The provisions of the Administrative Affairs Courts Law, 2000, shall apply to proceedings under this section with necessary changes; the Minister of Justice, with the approval of the Constitution Committee, may establish provisions regarding procedural rules in proceedings under this section; until such provisions are established, the provisions of the Citizenship Regulations (Procedural Rules for Citizenship Revocation Request), 2017, shall apply with necessary changes.

### Judicial Order to Cease Data Processing Operations or Delete Personal Data

### Chapter D: 4’ Enforcement Powers and Penalties

### Section A: Enforcement Powers

**23n. (a)** The head of the Authority may authorize an investigator from among state employees, who will be granted the powers under this law, in whole or in part (hereinafter - investigator), if all of the following are met:

The Israel Police has notified, within three months of the head of the Authority’s request, that it does not object to their authorization for reasons of public security, including due to their criminal record;

They have received appropriate training in the area of powers that will be granted to them under this law, and have met additional eligibility conditions, if any were set, as instructed by the Minister of Justice with the agreement of the Minister of National Security, and regarding the exercise of powers to access computer material or copy it as stated in section 23na(a)(3) - they hold a position skilled in performing such actions;

They have received appropriate training in the field of privacy protection, as instructed by the Minister of Justice.

**(b)** The authorization of an investigator under this section shall be in a certificate signed by the head of the Authority, which attests to their role as an investigator and their powers under this law (hereinafter - investigator certificate).

**(c)** Notice of authorization under subsection (b) shall be published in the Official Gazette and on the website of the Privacy Protection Authority.

### Authorization of Investigators

**23na. (a)** If an investigator had reasonable grounds to suspect that an offense was committed under section 5, under the circumstances listed in section 2(9), and the suspicion is that the offense was committed regarding information about a person’s private affairs in a database, or if an investigator had reasonable grounds to suspect that an offense was committed under Chapter B or under this chapter, they may -

Investigate any person connected to such offense or who may have knowledge related to such offense; the provisions of sections 2 and 3 of the Criminal Procedure Ordinance (Testimony) and the provisions of the Criminal Procedure Law (Interrogation of Suspects), 2002, shall apply to an investigation under this paragraph, with the necessary changes;

Seize any object that they have reasonable grounds to believe is an object related to such offense;

Request from the court a search and seizure warrant or a warrant to access computer material according to sections 23 to 24 of the Arrest and Search Ordinance, and execute it.

**(b)** The provisions of sections 23a, 24(a)(1) and (b), 26 to 28, 31 to 42 and 45, of the Arrest and Search Ordinance shall apply to the execution of a search, seizure of an object and access to computer material or its copying under this section, with the necessary changes, and with these changes: the powers granted to a police officer shall be granted to an investigator and the powers granted to an officer shall be granted to the head of the Authority or to an investigator they authorized for this purpose; notice of authorization under this subsection shall be published in the Official Gazette and on the Authority’s website.

**ג. (1)** If an investigator has reasonable grounds to suspect that a person has committed an offense as stated in subsection (a), they may detain them to verify their identity and address or to question them at their location. If identification is insufficient or the person cannot be questioned at their location, the investigator may require that person to accompany them to the Authority’s offices or summon them to the Authority’s offices at another time to be determined. A person summoned to the Authority’s offices shall appear at the time they were summoned.

Detention under paragraph (1) shall be subject to the provisions of sections 66, 67, and 72 to 74 of the Arrests Law, with necessary changes, and with these changes: The powers granted to a police officer shall be granted to an investigator, and the powers granted to the supervising officer shall be granted to the head of the Authority or to an investigator authorized by them, and the Authority’s offices that the head of the Authority has declared in a notice in the official gazette shall be considered as a police station for the purposes of the Arrests Law.

### Enforcement Powers

**23nb. (a)** An investigator shall not use the powers granted to them under this section except in the performance of their duties and when these two conditions are met:

The provisions regarding the identification of an inspector under section 23ia apply to them, with necessary changes;

They wear investigator uniforms, in the color and form ordered by the head of the Authority for this matter, provided that such uniforms do not appear to be police uniforms.

**(b)** The provisions of section 23ib(b) and (c) shall apply, with necessary changes, regarding the obligations mentioned in subsection (a).

### Investigator Identification

### Section B: Offenses

**23ng.** One who interferes with the head of the Authority, an investigator, or an inspector in the performance of their duties under this law, is liable to six months imprisonment.

### Interference with the Head of the Authority, Investigator, or Inspector in the Performance of Their Duties

**23nd.** One who does one of the following with the intention to mislead the head of the Authority, an inspector, or an external expert, is liable to two years imprisonment:

Includes incorrect details in an application for registration of a database submitted under section 9 or in a notice of change in the details listed in section 9(b) or in a notice under section 8a(b);

Provides incorrect details in response to a request from an inspector under section 23i(a)(1) to (3) or from an external expert under section 23ih(f).

### Misleading the Head of the Authority, Inspector, or External Expert

**23nh.** One who processes personal information from a database without authorization from the controller of the database, in violation of the provisions of section 8(c), is liable to three years imprisonment.

### Processing Information from a Database Without Authorization

**23nv.** One who approaches a person to obtain personal information for the purpose of processing the information in a database and provides them with incorrect details, in violation of the provisions of section 11, with the intention to mislead them regarding the provision of personal information, is liable to three years imprisonment.

### Providing Incorrect Information When Requesting Data

23nz. A public entity as defined in section 23 that is a corporation, an employee of such a public entity, or someone acting on behalf of such a public entity, who provides personal information whose transfer is prohibited under the provisions of section 23b, with the intention that an unauthorized party will process it, is liable to three years imprisonment.

### Unlawful Disclosure of Information from a Public Entity

### Chapter D:5 Provisions Regarding Elections

23nh. In this chapter –

“General elections for local authorities” – The general elections as defined in section 4 of the Local Authorities (Elections) Law;

“Elections for local authority” – Elections as defined in the Local Authorities (Elections) Law or in the Regional Councils (Date of General Elections) Law, 1994, except for elections to the local committee of a settlement in a regional council;

“Central Elections Committee” – As defined in the Knesset Elections Law [Consolidated Version], 1969;

“Elections (Propaganda Methods) Law” – Elections (Propaganda Methods) Law, 1959;

“Regional Councils Law” – Regional Councils (Election of Head of Council) Law, 1988;

“Local Authorities (Elections) Law” – Local Authorities (Elections) Law, 1965;

“Chairman of Regional Elections Committee” – Chairman of a Regional Elections Committee appointed under section 17d of the Elections (Propaganda Methods) Law, regarding elections for a local authority in the jurisdiction of the district court in which he serves;

“Candidate in local authority elections” – Any of the following:

From the beginning of the general elections period for local authorities until the day of submitting lists:

A party as defined in the Local Authorities (Elections) Law and a Knesset faction;

A faction of an outgoing council, as defined in section 25 of the Local Authorities (Elections) Law;

Anyone entitled, under section 16(b)(1) of the Local Authorities (Elections) Law, to receive voter registry information, and the information was provided to them under section 16(c) of said law;

Anyone entitled, under section 5b(a)(1) of the Regional Councils Law, to receive voter registry information, and the information was provided to them under said section;

From the day of submitting candidate lists – A list of candidates in elections for the council of a local authority and a candidate for head of a local authority, as well as whoever submitted the list of candidates or the candidate proposal, except for a group of voters;

“Party” - as defined in the Political Parties Law, 1992, and for the part of the Knesset election period beginning on the day after the last date for submitting a list of candidates for the Knesset to the Central Elections Committee - a party that has submitted a list of candidates participating in the Knesset elections;

“Election periods” - the Knesset election period or the general local authority election period;

“General local authority election period” - a period beginning on the 101st day before the general local authority election day, and ending on the 14th day after the said election day;

“Knesset election period” - a period beginning on the determining day, as defined in the Party Financing Law, 1973, and ending on the day of publication of the election results according to Section 11 of the Basic Law: The Knesset;

### Chapter D5 - Definitions

“Local authority election period” - a period beginning on the day of submission of candidate lists or candidate proposals and ending on the 14th day after the election day.

23T. (a) The head of the authority, inspector, or investigator shall not, during election periods, exercise authority granted to them under the sections listed below due to violation of provisions under this law, relating to a database in which a party or a candidate in local authority elections are the controlling owners, which they or someone holding such a database on their behalf have carried out, unless they have received approval according to subsection (b):

Entry to a place, according to Section 23J(a)(4);

Submitting a request for a search and seizure warrant or a computer material penetration warrant as part of an administrative inquiry, according to Section 23N;

Submitting a request for a cessation order, according to Section 23M;

Authority to seize any object, according to Section 23NA(a)(2);

Submitting a request for a search and seizure warrant or a computer material penetration warrant, according to Section 23NA(a)(3);

Notice of intent to charge according to Section 23K;

Delivering an administrative warning, according to Section 23L;

Delivering a notice on the possibility to submit a letter of commitment and deposit a bond, according to Section 23M.

(b) Authority as stated in subsection (a) may be exercised -

During a Knesset election period, regarding a database in which a party is the controlling owner - with the approval of the Chairman of the Central Elections Committee;

During a general local authority election period, regarding a database in which a party as defined in the Local Authorities (Elections) Law or a Knesset faction is the controlling owner - with the approval of the Chairman of the Central Elections Committee, and regarding a database in which another candidate in local authority elections is the controlling owner - with the approval of the Chairman of a Regional Elections Committee.

(ג) Before granting approval under this section, the chairman of the Central Elections Committee or the chairman of the Regional Elections Committee, as applicable, shall give the party or candidate in the local authority elections concerned an opportunity to present their arguments; however, regarding authority under subsection (a)(1) to (5), the chairman of an elections committee as stated may grant approval to exercise the authority without requesting the position of the party or candidate in the local authority elections, for reasons of urgency or if doing so would thwart the purpose of exercising the requested authority; the circumstances of the matter and reasons for urgency shall be detailed in the chairman’s decision.

(ד) The chairman of the Central Elections Committee or the chairman of a Regional Elections Committee shall not grant approval to exercise authority under this section if he finds that it would substantially impair the ability of the party or candidate in the local authority elections, as applicable, to compete in the elections or manage their relationship with the voting public, and that the expected severity of such harm outweighs the risk of privacy infringement and the risk of harm to the public interest underlying the exercise of authority; such approval may be conditional.

(ה) The chairman of the Central Elections Committee and the chairman of a Regional Elections Committee hearing a particular request may, on their own initiative or upon request of a party submitted before or during the hearing, order that the hearing be held before the chairman of the Central Elections Committee, if they see that it is justified under the circumstances.

(ו) If the head of the authority, supervisor or investigator decides to exercise authority under this section during an election period for a local authority held on a day other than the general election day for authorities, regarding a database in which the candidate in the local authority elections is the controlling owner, the candidate in the local authority elections may request from the chairman of a Regional Elections Committee, and if it is a party as defined in the Local Authorities (Elections) Law or a Knesset faction - from the chairman of the Central Elections Committee, to determine that said authority shall not be exercised during the election period for that local authority, if he finds that the provisions of subsection (d) apply, or to make the exercise of authority conditional; the provisions of subsections (c) and (e) shall apply to such request and decision, with the necessary changes.

### Exercise of powers under Chapters D1 and D3 during election periods

(ז) The provisions of sections 17d and 17e of the Elections (Propaganda Methods) Law shall apply to proceedings under this section, with the necessary changes.

### Translate the document

(h) The provisions of this section shall apply, mutatis mutandis, also to elections for another local authority or another regional council funded from the state budget, except for a local committee.

### Cancellation of Statute of Limitations

26. The statute of limitations for a civil claim under this law is two years.

### Cancellation

31a. (a) A person who does one of the following is liable to one year imprisonment:

Manages, holds or uses a database contrary to the provisions of section 8;

Provides incorrect details in an application for registration of a database as required in section 9;

Does not provide details or provides incorrect details in a notice accompanying a request to receive information under section 11;

Does not comply with the provisions of sections 13 and 13a regarding the right to review information held in a database, or does not correct information according to the provisions of section 14;

Allows access to a database contrary to the provisions of section 17a(a) or does not submit documents or an affidavit to the registrar in accordance with the provisions of section 17a(b);

Does not appoint a person responsible for information security in accordance with the provisions of section 17b;

Manages or holds a database used for direct mailing services, contrary to the provisions of sections 17d to 17f;

Discloses information contrary to sections 23b to 23e.

(b) An offense under this section does not require proof of criminal intent or negligence.

### Penalties for Strict Liability Offenses

36. The Minister of Justice is responsible for the implementation of this law and may, with the approval of the Constitution, Law and Justice Committee of the Knesset, make regulations on any matter relating to its implementation, including -

Conditions for holding and storing information in databases;

Conditions for transferring information to or from databases outside the state borders;

Rules of conduct and ethics for owners, controllers or managers of databases and their employees;

Provisions regarding the destruction of information upon cessation of operation of a database.

### Implementation and Regulations

36a. (a) The Minister of Justice, with the approval of the Constitution, Law and Justice Committee of the Knesset, may determine fees for reviewing databases under this law.

### Fees

(b) Fees collected under this section shall be allocated to the registrar and the supervision unit for their operations under this law.

(c) If the periodic fee or additional fee to the periodic fee, as applicable, is not paid within six months from the date set in the regulations for payment of the additional fee, the registration of the database in the registry will be suspended until payment.

36b. The Minister of Justice may, by order, with the approval of the Constitution Committee, amend the Third Schedule, the Fourth Schedule and the Fifth Schedule.

### Amendment of Schedules

### First Schedule

(The definition of “The Authority," “The Privacy Protection Authority," in Section 3)

Text of Government Decision No. 1890

Subject of Decision: Independence of the Privacy Protection Authority and Amendment of Government Decision

Decide:

Following Government Decisions No. 4660 of January 19, 2006, No. 4820 of June 28, 2012 and No. 3019 of September 7, 2017:

(a) The Privacy Protection Authority (hereinafter: the Authority) is a unit in the Ministry of Justice headed by the Head of the Authority.

(b) The Authority shall be independent in exercising the powers vested in the Head of the Authority for the fulfillment of its duties through the Authority’s employees and in accordance with any law, and the Authority’s operating budget shall be managed separately within the Ministry of Justice’s budget. Out of respect for the Authority’s independence, the Authority shall act independently when exercising the powers vested in the Head of the Authority.

The duties of the Authority include, among others:

To supervise compliance with the provisions of the Privacy Protection Law, 1981 and its regulations regarding databases;

To investigate suspicions of offenses under the Privacy Protection Law, 1981 regarding databases in accordance with its legal powers;

To raise public awareness of the right to privacy in databases, the value of privacy protection and its importance in the information age, through education, training and explanation;

To handle substantial public inquiries regarding harm to data subjects under the Privacy Protection Law, 1981;

To develop and implement professional programs and training in its areas of activity;

To promote and maintain relations with parallel bodies worldwide and within international forums in which parallel bodies participate;

To carry out the powers of the Registrar of Certifying Authorities under the Electronic Signature Law, 2001.

(a) Following Government Decisions No. 4660 of 19.1.2006 and No. 3543 of 11.2.2018, to determine that the qualifications for appointment as Head of the Authority shall be as follows:

One who meets the qualifications for appointment as a judge of the District Court;

**Translation:**

A person who has been convicted of a criminal offense or disciplinary offense which, due to its nature, severity, or circumstances, makes them unfit to serve as head of the Authority, or against whom an indictment or complaint has been filed for such an offense and a final judgment has not yet been given in their case, shall not be appointed as head of the Authority.

(b) It should be clarified that in accordance with Government Decision No. 4470 dated 8.2.2009, the head of the Authority shall be appointed for a single term of six years.

To amend Government Decision No. 4660 dated 19.1.2006 and determine that:

The government shall appoint the head of the Authority by notice in the Official Gazette as a registrar for the purpose of Section 7 of the Privacy Protection Law, 5741-1981;

The Minister of Justice shall appoint the head of the Authority as a registrar for the purpose of Section 9 of the Electronic Signature Law, 5761-2001.

### Second Addendum

(Paragraph (12) of the definition of “information of special sensitivity” in Section 3)

Information on membership in a workers’ organization as stated in Regulation 7 of the Privacy Protection Regulations (Provisions regarding information transferred to Israel from the European Economic Area), 5783-2023.

### Third Addendum

(Section 23Co(h))

Financial sanction for violation of information security regulations

In this addendum - “External entity” - as defined in Regulation 15(a) of the regulations;

“Individual” - a person and their relative, a person and their representative; for this purpose, “relative” - spouse, sibling, parent, grandparent, descendant and descendant of a spouse, and the spouse of any of these, as well as a descendant of a sibling, and a sibling of a parent;

“Database managed by an individual” - a database whose controller is an individual or a corporation owned by an individual or a corporation owned by two individuals, and at most two additional authorized persons are permitted to use it and are able to use it, excluding databases as detailed below:

A database whose main purpose is collecting personal information for the purpose of transferring it to another as a business or for consideration, including direct mailing services;

A database that contains personal information about 10,000 or more individuals;

A database containing personal information for which the database owner is subject to professional confidentiality by law or by principles of professional ethics;

“Database subject to basic security level” - a database that is not managed by an individual and meets all of the following:

Its main purpose is not collecting personal information for the purpose of transferring it to another as a business or for consideration, including direct mailing services;

The controller of the database is not a public body as defined in Section 23;

If the database contains information of special sensitivity, one of the following also applies:

The number of authorized persons for the database at the controller does not exceed ten;

### Translate the document

**(b)** The database includes particularly sensitive information only about employees of the controller or its suppliers, it is used solely for managing the business of the database controller and is only of the following types:

Information according to paragraphs (2), (6) and (8) to (10) of the definition of “particularly sensitive information”;

Personal information about the sexual orientation of the employee or their spouse, derived from information provided by the employee;

Personal information about religious beliefs;

Personal information that is biometric identifier as stated in paragraph (4) of the definition of “particularly sensitive information” which is only a facial image;

**“Database subject to medium security level”** - a database that is not managed by an individual and is not subject to high security level, and meets one of the following:

Its main purpose is collecting information for transfer to others as a business or for compensation, including direct mailing services;

Its controller is a public body as defined in section 23 of the law;

The database contains particularly sensitive information, except for particularly sensitive information excluded in paragraph (3)(b) of the definition of “database subject to basic security level”;

**“Database subject to high security level”** - a database that meets one of the following:

A database as stated in item (1) of the definition of “database subject to medium security level” or a database containing particularly sensitive information where the number of authorized personnel at the controller exceeds 100 or it contains personal information about 100,000 or more individuals;

A database that contains biometric identifiers of 100,000 or more individuals;

**“Information Security Regulations”** - Privacy Protection Regulations (Information Security), 2017.

### Amount of monetary sanction (in New Israeli Shekels) | The violation

Column E Database | subject to high | security level | Column D Database | subject to medium | security level | Column C Database | subject to basic | security level | Column B Database | managed by an individual | Column A

160,000 | 40,000 | 2,000 | 2,000 | (1) Preparing database definition document: A database controller who did not define in the database definition document all matters stated in regulation (2a) of the Information Security Regulations, in violation of the provisions of that regulation, including the different types of information included in the database according to sub-regulation (3), with attention to the list of information types constituting particularly sensitive information according to section 3 of the law

Updating database definition document: A database controller who did not update the database definition document, contrary to the provisions of Regulation (2b) of the Information Security Regulations

160,000 | 40,000 | 2,000 | 2,000

Checking excess information: A database controller who did not examine or document the examination of whether the information stored in the database is more than necessary for the purposes of the database, contrary to the provisions of Regulation (2c) or (19b) of the Information Security Regulations

160,000 | 40,000 | 2,000 | 2,000

Preparation of information security procedure: A database controller or database holder who did not establish in a document an information security procedure in accordance with the database definition document and information security regulations (hereinafter - security procedure), contrary to the provisions of Regulation (4a) of the Information Security Regulations or the provisions of said regulation as applied in Regulation (19a) of said regulations, as applicable

160,000 | 40,000 | 2,000 | –

Security procedure - preparation, preservation and determination of provisions: A database controller or database holder who did not do one of the following:

Preserved the security procedure so that details from it are provided to authorized persons only to the extent required for the performance of their duties, contrary to the provisions of Regulation (4b) of the Information Security Regulations or the provisions of said regulation as applied in Regulation (19a) of said regulations, as applicable;

Included in the security procedure the details listed in Regulation (4c) of the Information Security Regulations; and regarding a database subject to medium or high security level - included reference to the details listed in Regulation (4d) of the Information Security Regulations or the provisions as stated in Regulation (9b)(2) of the Information Security Regulations or the provisions of said regulation as applied in Regulation (19a) of said regulations, as applicable;

Established in the security procedure provisions regarding dealing with information security incidents or reporting to the database controller, contrary to the provisions of Regulation (11b) of the Information Security Regulations or the provisions of said regulation as applied in Regulation (19a) of said regulations, as applicable;

Detailed in the security procedure the matters listed in Regulation (15a)(2)(a) to (e) of the Information Security Regulations, contrary to the provisions of Regulation (15a)(3) of said regulations

160,000 | 40,000 | 2,000 | –

Structure of the database and its systems: A database controller or database holder who did not maintain an updated document of the database structure or an updated inventory list of the database systems, in accordance with the provisions of Regulation (5a) of the Information Security Regulations or the provisions of said regulation as applied

80,000 | 20,000 | 1,000 | –

Providing database structure details and inventory list: 80,000 | 20,000 | 1,000 | –

A database controller or processor who did not maintain the updated document of the database structure or the inventory list according to access permissions set in accordance with the provisions of Regulation 5(b) of the Information Security Regulations or the provisions of said regulation as applied in Regulation 19(a) of the aforementioned regulations, as applicable

System protection: 80,000 | 20,000 | 1,000 | 1,000

A database controller or processor who did not ensure that the systems specified in Regulation 5(a)(1) of the Information Security Regulations are kept in a protected place, preventing unauthorized entry and access, in a manner consistent with the nature of the database activity and the sensitivity of the information therein, in accordance with the provisions of Regulation 6(a) of the Information Security Regulations or the provisions of said regulation as applied in Regulation 19(a) of the aforementioned regulations, as applicable

Risk survey: 320,000 | – | – | –

A database controller or processor who did not ensure that a survey to identify information security risks is conducted at least once every 18 months (hereinafter - risk survey), or did not discuss the results of the risk survey submitted to him and did not examine the need to update the database definition document or security procedure as a result, or did not act to correct the deficiencies revealed in the risk survey, contrary to the provisions of Regulation 5(c) of the Information Security Regulations or the provisions of said regulation as applied in Regulation 19(a) of the aforementioned regulations, as applicable

Penetration tests: 320,000 | – | – | –

A database controller or processor who did not ensure that penetration tests of the database systems are conducted at least once every 18 months, or did not discuss the results of the penetration tests or did not act to correct the deficiencies revealed, contrary to the provisions of Regulation 5(d) of the Information Security Regulations or the provisions of said regulation as applied in Regulation 19(a) of the aforementioned regulations, as applicable

Control and documentation of site entry: 80,000 | 20,000 | – | –

A database controller or processor who did not take measures for control and documentation in accordance with the provisions of Regulation 6(b) of the Information Security Regulations or the provisions of said regulation as applied in Regulation 19(a) of the aforementioned regulations, as applicable

Human resource management: 80,000 | 20,000 | 1,000 | –

A database controller

Staff training: A database controller or processor who granted access to information in the database or changed the scope of authorization given, without conducting prior training or providing required information to authorized individuals, in violation of regulation 7(b) of the Information Security Regulations or

(19) Documentation of information security incidents: A database controller or processor who did not ensure documentation of every case where an incident was discovered raising concerns about data integrity, unauthorized use, or exceeding authorization (hereinafter - information security incidents), in violation of regulation 11(a) of the Information Security Regulations or the provisions of said regulation as applied in regulation 19(a) of said regulations, as applicable

(20) Periodic discussion of information security incidents: A database controller or processor who did not hold a discussion on information security incidents or did not examine the need to update the security procedure and document such discussion and examination, in violation of regulations 11(c) and 19(b) of the Information Security Regulations or the provisions of said regulation as applied in regulation 19(a) of said regulations, as applicable

(21) Reporting to the Authority about a severe security incident: A database controller or processor who did not immediately notify the head of the Authority about a severe security incident, or did not report to the head of the Authority about the steps taken following the incident, in violation of regulation 11(d)(1) of the Information Security Regulations or the provisions of said regulation as applied in regulation 19(a) of said regulations, as applicable

(22) Updating database systems: A database controller or processor who did not ensure that ongoing updates are made to the database systems, including computer material required for their operation, or that systems not supported by the manufacturer in security aspects are not used without any

(23) Network connection security: A database controller or processor who connected the database systems to the Internet or another public network without installing all protective measures, in violation of regulation 14(a) of the Information Security Regulations or the provisions of said regulation as applied in regulation 19(a) of those regulations, as applicable

160,000 | 40,000 | 2,000 | 2,000

(24) Control and supervision of external entity (outsourcing): A database controller who contracted with an external entity for the purpose of receiving a service, who did not explicitly stipulate in the agreement with the external entity the matters listed in regulation 15(a)(2) of the Information Security Regulations or did not take any control and supervision measures regarding the external entity’s compliance with the provisions set in said agreement on the matters detailed in sub-paragraphs (d) and (f) to (h) of said regulation, in violation of regulation 15(a)(4) of the Information Security Regulations

320,000 | 80,000 | 4,000 | –

(25) Documentation: A database controller or processor who did not securely retain, for at least one year, the data accumulated in the implementation of the provisions of regulations 6(b), 8 to 11, 14, 15(a)(4) and 16 of the Information Security Regulations applicable to them, in violation of regulation 17(a) of the Information Security Regulations or the provisions of said regulation as applied in regulation 19(a) of the Information Security Regulations, as applicable

80,000 | 20,000 | 1,000 | –

(26) Backup of documentation data: A database controller or processor who did not do one of the following:

80,000 | 20,000 | – | –

Backed up the stored data in a manner that ensures it can be restored to its original state at any time, contrary to the provisions of Regulation 17(b) of the Information Security Regulations or the provisions of said regulation as applied in Regulation 19(a) of said regulations, as applicable;

Specified in a document the matters listed in Regulation 18(a)(1) and (3) of the Information Security Regulations and established procedures to ensure data recovery, as stated in Regulation 17(b) of said regulations;

Ensured that a backup copy of the data and procedures mentioned in Regulation 18(a) of the Information Security Regulations is kept in a manner that ensures the integrity of the information and the possibility of information recovery, contrary to the provisions of Regulation 18(b) of the Information Security Regulations or the provisions of said regulation as applied in Regulation 19(a) of said regulations, as applicable

(27) Violation of documentation obligations: A database controller or database holder who did not document the manner of performing an action that is not the creation of a document, which they have an obligation or responsibility to perform according to the regulations, contrary to the provisions of Regulation 19(b) of said regulations

(28) Separation of database systems (compartmentalization): A database controller or database holder who did not separate between database systems from which personal information can be accessed and other computer systems used by them, contrary to the provisions of Regulation 13(b) of the Information Security Regulations or the provisions of said regulation as applied in Regulation 19(a) of said regulations, as applicable

(29) Periodic review: A database controller or database holder who did not ensure that an internal or external audit is conducted at least once every 24 months, contrary to the provisions of Regulation 16(a) of the Information Security Regulations or the provisions of said regulation as applied in Regulation 19(a) of said regulations, as applicable, or who did not discuss the audit reports submitted to them, or did not examine the need to update the database definition document or security procedure following them, contrary to the provisions of Regulation 16(c) of the Information Security Regulations or the provisions of said regulation as applied in Regulation 19(a) of said regulations, as applicable

### Fourth Appendix

(Section 23ko(i))

Monetary sanction for violation of regulations on transferring information from the European Economic Area

In this appendix, “Regulations on transferring information from the European Economic Area” - Privacy Protection Regulations (Provisions regarding information transferred to Israel from the European Economic Area), 2023.

### Part A

Column B: Amount of monetary sanction | Column A: The violation

### 15,000 New Shekels

A controller of a database who did not notify in writing to the data subject about their decision on a request according to the provisions of regulation (3a) of the Regulations on Transfer of Information from the European Economic Area, in violation of the provisions of regulation (3d) of the said regulations

An amount of 2 New Shekels for each person whose personal information is in the database, and if the personal information in the database was information of special sensitivity - an amount of 4 New Shekels for each person; If the amount of the monetary sanction was less than 20,000 New Shekels, and if the said information was of special sensitivity - less than 40,000 New Shekels, the head of the Authority may impose on the controller of a database or on a holder of a database a monetary sanction in the amount of 20,000 New Shekels or 40,000 New Shekels, as applicable

A controller of a database who did not operate any organizational, technological or other mechanism, aimed at ensuring that the database does not hold information that is no longer necessary for the purpose for which it was collected or held or for another purpose for which it is permitted to hold it according to any law (hereinafter - unnecessary information), in violation of the provisions of regulation (4a) of the Regulations on Transfer of Information from the European Economic Area

A controller of a database who did not operate any organizational, technological or other mechanism aimed at ensuring that the information in the database is correct, complete, clear and up-to-date, in violation of the provisions of regulation (5a) of the Regulations on Transfer of Information from the European Economic Area

A controller of a database who found that the database holds information that is not correct, complete, clear or up-to-date, and did not take any measures to correct or delete the information, in violation of the provisions of regulation (5b) of the Regulations on Transfer of Information from the European Economic Area

### Part B

Column B: Amount of Monetary Sanction | Column A: The Violation

A sum of 4 New Israeli Shekels for each person whose personal information is found in the database, and if the personal information in the database was particularly sensitive information - a sum of 8 New Israeli Shekels for each person; If the amount of the monetary sanction was less than 200,000 New Israeli Shekels, the head of the Authority may impose on the database controller or processor a monetary sanction in the amount of 200,000 New Israeli Shekels; Regarding items (1), (3) and (4) - the monetary sanction will be calculated according to the number of people whose personal information the controller did not delete as required or did not notify them as required in regulation (3c) or (6a) or (6b) of the European Economic Area Data Transfer Regulations, as applicable:

A database controller who received a written request to delete personal information as stated in regulation (3a) of the European Economic Area Data Transfer Regulations, and the exceptions stated in regulation (3b) of said regulations did not apply, and he did not delete the information or perform actions ensuring that it would not be possible, by reasonable means, to identify the data subject, in violation of the provisions of regulation (3c) of said regulations, after receiving a notice from the head of the Authority according to section 23kh(c), that his actions constitute a violation, and did not stop the violation within the period ordered by the head of the Authority

A database controller who found that personal information that is not necessary according to regulation (4b) of the European Economic Area Data Transfer Regulations is held in the database and did not perform actions ensuring that it would not be possible to identify the data subject as stated in regulation (4c) and the circumstances set in said regulation did not exist, and did not delete said information at the earliest possible time under the circumstances, in violation of the provisions of regulation (4b) of said regulations, after receiving a notice from the head of the Authority according to section 23kh(c) that his actions constitute a violation, and did not stop the violation within the period ordered by the head of the Authority

A database controller who received personal information about a person and did not notify him as required in regulation (6a) of the European Economic Area Data Transfer Regulations, and none of the circumstances set in regulation (6c) of said regulations existed, in violation of said regulation (6a), after receiving a notice from the head of the Authority according to section 23kh(c) that his actions constitute a violation, and did not stop the violation within the period ordered by the head of the Authority

**Translate the document**

### (4)

A controller of a database who wished to transfer the personal information received to a third party and did not notify the data subject as required by regulation (6b) of the regulations for transferring information from the European Economic Area, and none of the circumstances specified in regulation (6c) of the said regulations were met, in violation of the said regulation (6b), and this after receiving a notice from the head of the Authority according to section 23kh(c) that his actions constitute a violation, and did not stop the violation within the period ordered by the head of the Authority

### Fifth Addendum

(Section 23l)

### Reduced Amounts for Financial Sanctions

In this addendum -

“Approval regarding the amount of turnover” - as detailed below, as applicable:

For a violator required by law to appoint an auditor as defined in the Companies Law, 1999 - approval given by the auditing accountant;

For a violator that is a cooperative society - approval of the person who audited the accounts of the cooperative society according to section 20 of the Cooperative Societies Ordinance;

For another violator - approval given by an accountant or a representing tax advisor, that the amount of turnover presented by the violator corresponds to what is stated in a document submitted to the Israel Tax Authority or to the National Insurance Institute according to law; For this purpose, “representing tax advisor” - as defined in the Regulation of Tax Representation Law, 2005;

“Turnover” - turnover of a dealer as defined in the Value Added Tax Law, 1975; For a non-profit organization as defined in the said law - turnover as defined in the Second Addendum to the Associations Law, 1980, and for a public body that is not one of the aforementioned - the annual budget of that public body;

“Micro business” - a violator whose turnover in the year preceding the date of violation did not exceed 4 million new shekels;

“Small business” - a violator, except for a micro business, whose turnover in the year preceding the date of violation exceeded 4 million new shekels and did not exceed 10 million new shekels.

### Definitions

The head of the Authority will reduce for the violator the amount of the financial sanction in the rates detailed below, if one or more of these circumstances occurred:

In the five years preceding the violation of the provision for which a financial sanction is imposed on the violator, no financial sanction or administrative enforcement measure was imposed on him under signs B to E in Chapter D3 for violating the same provision - at a rate of 20%; and if in the three years preceding the violation no financial sanction or administrative enforcement measure was imposed on the violator as stated - at a rate of 10%;

The violator stopped the violation on his own initiative and reported it to the head of the Authority - at a rate of 30%;

The violator took actions to prevent recurrence of the violation and to reduce damage, to the satisfaction of the head of the Authority - at a rate of 20%;

The violator is obligated to appoint a privacy protection officer according to section 17b(1a)(3) and (4) only, and appointed such an officer before the notice of intent to charge was delivered - at a rate of 10%; Such reduction shall apply as long as the Minister of Justice, with the approval of the Constitution Committee, has not issued an order under section 23ko(d)(1)(g).

### Reduction due to the violator’s behavior

The head of the Authority may reduce the amount of the monetary sanction for the violator due to compensation paid or ruled against the violator for the same violations - at a rate not exceeding 30%.

### Reduction due to payment or other compensation paid

If the head of the Authority sees, regarding a violator who is an individual, that the violation was caused due to personal circumstances that justify a reduction of the monetary sanction or that severe personal circumstances existed that justify not exhausting the law with the violator, he may reduce the amount of the monetary sanction imposed on the violator at a rate of 20%.

### Reduction due to personal circumstances

If several circumstances as stated in sections 2, 3 and 4 apply to a violator, the head of the Authority may reduce the amount of the monetary sanction imposed on him by the rates listed alongside those circumstances, cumulatively, provided that the cumulative reduction rate does not exceed 70% of the amount of the monetary sanction.

### Reduction due to several circumstances

If the head of the Authority finds, at the request of the violator, that the violator is a micro or small business, as applicable, he will reduce the amounts of sanctions to be imposed on it, whether reduced according to section 2, 3 or 4 or not reduced as stated, so that the amount of the sanction for violations according to each of the paragraphs detailed below, will not exceed the amount specified alongside them:

### Reduction for micro or small business

For violations listed in section 23ko(a) and (b), in items (6) to (8), (11) to (14) and (25) to (28) of the Third Schedule, and item (1) in Part A of the Fourth Schedule:For a micro business - 20,000 new shekels, and for a small business - 40,000 new shekels

For violations listed in section 23ko(c) to (f), in items (1) to (5), (9) and (10), (15) to (24) and (29) of the Third Schedule, in items (2) to (4) of Part A of the Fourth Schedule and in Part B of the said Schedule:For a micro business - 50,000 new shekels, and for a small business - 100,000 new shekels

For violations listed in section 23ko(g):For a micro business - 70,000 new shekels, and for a small business - 140,000 new shekels

Reduction due to taking into account transaction turnover

If the violator is a micro or small business that has committed multiple violations according to paragraphs (1) to (3) - the violator shall not bear an amount exceeding the highest monetary sanction among the paragraphs.

(a) If the head of the authority finds, at the request of the violator, that the amount of the monetary sanction imposed on the violator, whether reduced according to sections 2, 3, 4 or 6 or not reduced as stated, exceeds 5% of the violator’s transaction turnover, he shall reduce the amount of the monetary sanction to 5% of his transaction turnover; however, for a business that has no transaction turnover, the head of the authority shall not reduce the amount of the sanction under this section to an amount less than the maximum amount that can be imposed according to section 6 regarding a micro business.

(b) A violator requesting a reduction of the monetary sanction amount according to section 6 or this section shall submit to the head of the authority a certification regarding the amount of his transaction turnover within 30 days from the date of delivery of the notice of intent to charge.