We, at Or-Hof Law, have created this English translation of the Privacy Protection Law 5741-1981, with an effort to closely mirror the original Hebrew version. We hope that you will find it useful. Hebrew is a gendered language, and the translation retains the masculine form when addressing all genders. The translation is available to everyone and made for general use including research, education, and commercial purposes, but it is not and should not be relied upon or construed as legal opinion or any other professional advice. The only official version of the law is the Hebrew version. We provide the translation "As-Is" without any warranty or guarantee of any kind, express or implied. If you have any questions or comments regarding the translation, please contact us at: office@or-hof.com. When you make available, publicly display, or distribute the translation, please keep this notice, do not change the document structure, and do not modify the translation. Thank you.

# Privacy Protection Law, 5741-1981

## CHAPTER A: Invasion of Privacy



## CHAPTER B: Protection of Privacy in Databases

### Subchapter A: Databases

# The Privacy Protection Law, 5571-1981

## CHAPTER A: Invasion of Privacy

1. Prohibition of Invasion of Privacy

A person shall not invade the privacy of another without his consent.

2. What is a Privacy Invasion

A privacy invasion includes one of the following:

(1) Spying on or trailing a person in a manner that may harass him or any other harassment;

(2) Eavesdropping that is prohibited by law;

(3) Photographing a person while he is in a private domain;

(4) Publication of a person's photograph to the public under circumstances that the publication may humiliate or disgrace him;

(4A) Publication of a photograph of an injured person to the public, that was taken at the time of the injury or shortly after, in such a way that he can be identified and in circumstances that the publication may embarrass him, except for the publication of a photograph without delay between the moment of photographing to the actual broadcasting moment, which does not exceed what is reasonable under those circumstances; for this purpose, "injured" means one who suffered physical or mental injury due to a sudden event and that the injury is visible;

(5) Copying the content of a letter or any other writing not intended for publication, or the use of its content, without the permission of the recipient or writer, provided that the document is not of historical value and fifteen years have not passed since its writing; for this purpose, "writing" includes electronic messages as defined in the Electronic Signature Law, 5761 – 2001;

(6) The use of a person's name, appellation, photograph, or voice for profit;

(7) Violating confidentiality obligations provided by law regarding a person's private affairs;

(8) Infringing confidentiality obligations regarding a person's private affairs, provided explicitly or implicitly in an agreement;

(9) The use of knowledge about a person's private affairs or delivering it to another, in a way that does not align with the purpose for which it was given;

(10) The publication or delivery of anything obtained through a privacy invasion in accordance with paragraphs (1) to (7) or (9);

(11) The publication of a matter concerning the privacy of a person's intimate life, including his sexual history, state of health, or behavior in the private domain.

2A. Publication of a Photograph of the Deceased

(a) For the purposes of this law, the publication to the public of a photograph of a person's visible corpse in a way that can be identified is considered a privacy invasion, unless one of the following applies:

(1) The person consented during his lifetime to the said invasion;

(2) 15 years have passed since the person's death;

(3) Consent to the said invasion was obtained from the first of the specified individuals in paragraphs (a) to (d) who is still alive, provided the deceased did not object to the said invasion during his lifetime, and his child or parent did not inform the publisher or to another publisher's behalf, of his objection to the publication:

(a) His spouse;

(b) Any of his children;

(c) His parents;

(d) Any of his siblings;

(4) The deceased had no family members listed in paragraph (3) and the court has approved the publication.

(b) A deceased person's spouse, child, parent, or sibling may file a civil lawsuit for a publication in accordance with this section.

3. In This Law –

"data Security" – protecting the integrity of personal data, or protecting personal data from processing, without lawful permission;

"person" – for the purposes of sections 2, 13, 14, 15a, 17b, 17b1, 17b2, 17f, 23b, 23m(f), and 25, and for the purposes of the definitions "direct mailing", "database", "biometric identifier", "personal data", and "data of special sensitivity" – excluding a body corporate;

"database controller" – the one who determines, alone or with another, the purposes of processing the data that is in the database, or an entity or an officer in that entity authorized by law to process data in the database;

"direct mailing" – contacting a person personally, based on his belonging to a population group that is determined by one or more characteristics of individuals whose names are included in a database;

"late payment fees" and "new shekel interest rate" – as defined in the Statutory Interest Rate and Linkage Adjudication Law, 5721 – 1961;

"consent" – the informed consent, obtained explicitly or implicitly;

“constitution committee” – the Constitution, Law, and Justice Committee of the Knesset;

“computer material”, “computer”, and “output” – as defined in the computers law;

“Regulation of security in public bodies” – Regulation of Security in Public Bodies Law, 5758-1998;

“freedom of information law” – Freedom of Information Law, 5758-1998;

"computers Law" – Computers Law, 5765-1995;

“arrests law” – Criminal Procedure (Enforcement Powers – Arrests) Law, 5756-1996;

“object” – as defined in the arrest and search ordinance;

“database” – a collection of personal data processed by digital means, except for one of the following:

1. A collection for personal use that is not for business purposes;
2. A collection that includes only a name, address, and contact details, regarding 100,000 individuals or less, which does not itself indicate additional personal data about the individuals whose names are included in it, provided that the owner of the collection or the body corporate under the owner’s control does not have another collection that includes other data details about the same individuals;

“biometric identifier” – a biometric datum used to identify a person or to verify that person’s identity, or a biometric measure from which the said datum can be derived; for the purposes of this definition, "biometric" – unique human, physiological, or behavioral characteristic that can be measured through computerized measurement;

“holder” – for the purpose of a database – an external entity to the database controller that is processing data on his behalf;

“personal data” – data relating to an identified or identifiable person; for the purposes of this definition, "identifiable person" one who can be identified with reasonable effort, directly or indirectly, including through an identifying detail such as name, identification number, biometric identifier, location data, online identifier, or one or more details relating to his physical, health, economic, social, or cultural status;

“data of special sensitivity” – any of the following:

(1) Personal data about a person's intimate family life, personal intimate affairs and sexual orientation;

(2) Personal data relating to a person's health status, including medical data as defined in the Patient Rights Law, 5756 – 1996;

(3) Personal data that constitutes genetic data as defined in the Genetic Information Law 5761 – 2000;

(4) Personal data that is a biometric identifier used or intended to be used to identify a person or verify his identity in a computerized manner;

(5) Personal data about a person's origin;

(6) Personal data about a person's criminal history;

(7) Personal data about a person's political opinions or religious beliefs or worldview;

(8) Personal data which is a personality assessment conducted by a professional entity that, as part of their occupation, expresses an opinion on a person's personality, or is conducted by means intended to perform an assessment of material personality traits, including character traits, intellectual competence, and ability to function at work or in studies;

(9) Personal data that is location data and transmission data, as defined in the Criminal Procedure Law (Enforcement Powers-Communication. Data) 5768 – 2007, created by an authorized provider as defined in the said law, regarding a person, and data about a person's location that can indicate data in accordance with paragraphs (1) to (7) and (11);

(10) Personal data about a person's payroll data and financial activity;

(11) Personal data subject by law to confidentiality obligations;

(12) Other personal data determined by the Minister of Justice, with the approval of the constitution committee, in schedule 2, provided that it is personal data in a database located in Israel that was transferred to it from outside the country and that in the place from which it was transferred, special legal provisions apply to such personal data compared to the law applicable to other personal data.

“database manager” – the database controller, and for a public body as defined in section 23 – the general manager of the body that owns or holds the database or one authorized by the general manager to manage the database;

"document" including output;

“inspector” – one who was authorized in accordance with the provisions of section 23i;

"registry" – the registry of databases as defined in section 12;

“system data” – data regarding the holding, management, and use of personal data and a database, provided that they do not include personal data;

“processing”, “use” – any action performed on personal data, including its receipt, collection, storage, copy, review, disclosure, exposure, transfer, delivery, or granting access to it;

"arrest and search ordinance" – Criminal Procedure (Arrest and Search) Ordinance [New Version], 5869 – 1969;

"publication" as defined in section 2 of the Prohibition of Defamation Law, 5725 – 1965;

"photographing" includes filming.

“head of the authority” – individual appointed by the government to lead the privacy protection authority and supervise the protection of personal data in databases in accordance with the provisions of this law;

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

“data integrity” – the identicality of data in a database to the source from which the data was obtained, without being changed, delivered, or destroyed without lawful permission.

4. Privacy Invasion – Civil Wrong

A private invasion is a civil wrong, and the provisions of the Torts Ordinance [New Version] shall apply to it subject to this law's provisions.

5. Privacy Invasion – Criminal Offence

Anyone who intentionally invades another's privacy in one of the ways mentioned in sections 2(1), (3) to (7), and (9) to (11), is subject to five years of imprisonment.

6. Trivial Act

There shall be no right to a civil or criminal claim under this law for insignificant harm.

## CHAPTER B: Protection of Privacy in Databases

7. (Revoked)

### Subchapter A: Databases

8. Database Management and Lawful Processing of Personal Data

(a) In this section, "processing" – except for incidental storage in good faith.

(b) No person shall process personal data in a database except for the lawfully established purpose of the database.

(c) No person shall process personal data from a database without authorization from the database controller or beyond the scope of the said authorization.

(d)

(1) A database controller shall not process personal data in a database or permit another to process such data on his behalf if the personal data contained in the database was created, received, accumulated, or collected in violation of this law or provisions of any other law that regulates data processing;

(2) If personal data was provided to a database controller by another entity, and the controller did not and could not have known that such entity acted unlawfully, the database controller shall not be liable under this subsection for processing personal data which was conducted before the database controller knew or should have known as aforesaid;

(3) The provisions of subsection (1) shall not apply to a minor violation of the law under the circumstances, and regarding personal data provided as mentioned in subsection (2), even if the controller knew or should have known.

8A. Registration or Notification Obligation

(a) (1) A database must be registered in the event of one of the following:

(a) Its main purpose is to collect personal data for providing it to another as a business practice or for consideration, including direct mailing services, and the database contains personal data about more than 10,000 individuals;

(b) The database controller is a public body as defined in subsection (1) of the definition "public body" in section 23, unless the database includes personal data on the public body's employees only;

(2) A database controller shall not process personal data in a database that is subject to registration and shall not permit another to process such data on his behalf, unless the database is registered in the registry; for this purpose, a database shall be deemed registered if the database controller submitted a registration application in accordance with the provisions of section 9 and the period mentioned in section 10(a)(1) has passed without the head of the authority notifying the applicant of his refusal to register the database or the suspension of the registration of the database;

(3) The head of the authority may exempt a database that is subject to registration from the registration obligation under subsection (1) if the head of the authority was convinced that the registration is not necessary to ensure compliance with this law regarding the database; The aforesaid notification shall be provided to the controller and published on the authority's website.

(b) (1) If the number of individuals that data of special sensitivity exists about them in a database which is not subject to registration under subsection (a)(1), exceeds 100,000, the database controller shall notify the authority, within 30 days of the aforesaid occurrence, the identity, address and contact details of the controller, the identity and contact details of the privacy protection officer – if the appointment thereof is required under section 17B1, and will provide the authority with a copy of the database definitions document the preparation of which is required under Regulations in accordance with sections 17(b) and 36;

(2) The controller mentioned in subsection (1) shall notify the authority, within 30 days of the date of the change or the cessation of the activity, as the case may be, of any change in the identity of the controller or the identity of the privacy protection officer and their contact details, on any change requiring an update to the database definitions document under the regulations in accordance with sections 17(b) and 36, and the cessation of the database activity;

(3) The minister of justice may prescribe Regulations regarding the notification methods in accordance with this subsection, and may also, with the approval of the constitution committee, exempt certain types of databases or controllers from the notification obligation.

(c) The provisions of this section shall not apply to a database containing only data that has been publicly published or made available to the public in accordance with a lawful authority.

9. Application for Registration

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

(b) The application for the registration of a database shall detail –

(1) The identity, the address in Israel and the contact details of the database controller, and the identity and contact details of the privacy protection officer;

(1A) The type of service provided by the database holder to the controller;

(2) The purposes of establishing the database and the purposes for which the data is intended;

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

(4) Details regarding the transfer of data outside the country's borders;

(5) Details regarding the receipt of data, regularly, from a public body as defined in section 23, the name of the public body providing the data and the nature of the data provided, except for details provided with the consent of the data subject.

(c) The Minister of Justice, with the approval of the constitution committee, may prescribe additional details to be included in the registration application.

(d) The database controller shall notify the head of the authority of any change in the details specified in subsection (b) or in accordance with subsection (c) and on the cessation of the database activity.

10. Powers of the Head of the Authority Regarding Database Registration

(a) if an application for the registration of a database was submitted–

(1) The head of the authority shall register it in the registry within 60 days of the application submission, unless the head of the authority had reasonable ground to assume that the database is used or may be used for illegal activities or as a guise for them, or that the personal data contained therein was created, received, accumulated, or collected in violation of this law or in violation of provisions of any law; however, if the head of the authority requested additional data and details from the applicant, the period until the submission of the aforesaid data and details will not be taken into account;

(2) The head of the authority may register a different purpose than the one specified in the application, register multiple purposes for the database, or order the database to be

registered as several separate databases, all of which if the head of the authority has realized that it suits the actual activity of the database;

(3) The head of the authority shall not refuse to register the database and will not exercise his power under subsection (2), unless he has provided the applicant an opportunity to present the applicant's arguments.

(b) (Revoked)

(b1) (Revoked)

(b2) If the head of the authority has notified the applicant of his refusal to register the database or of the suspension of the registration, the applicant shall not be permitted to process personal data in the database and will not permit another to process personal data in the database on the applicant's behalf, unless the court determined otherwise.

(b3) The head of the authority shall delete the registration of a database from the registry, if notified by the database controller that the data in that database was deleted or transferred to another registered database and no longer exists, or that the database is no longer subject to registration, and the database controller confirmed this statement by an affidavit.

(c) (Revoked)

(d) (Revoked)

(e) (Revoked)

(e1) (Revoked)

(f) If the database controller or database holder violated the provisions of this law or regulations under this law, or failed to comply with a demand directed to him by the head of the authority, the head of the authority may suspend the registration for a period of time which will be set by him, or cancel the registration of the database in the registry, if he was convinced that it is required under the circumstances, provided that prior to the suspension or the cancellation, the database controller or the database holder have been given an opportunity to present his arguments.

(g) (Revoked)

10A. (Revoked)

11. Obligations of a Data Requestor

A request from a person to receive personal data for the purpose of processing the personal data in a database shall be accompanied by a notice stating –

(1) If the person is subject to a legal obligation to provide the data, or if the provision of the data depends on the person's will and consent and the consequence of non-consenting;

(2) The purpose for which the data is requested;

(2a) The name and contact details of the database controller;

(3) To whom the data will be delivered and the purposes of delivery.

(4) The existence of the right to review the personal data in accordance with section 13 and the right to request correction of personal data in accordance with section 14.

12. Registry of Databases

(a) The head of the authority shall maintain a registry of databases, which shall be available for review by the public and shall enable search of details in it.

(b) The registry shall contain the details for the registration of the database as mentioned in section 9, except for the name of the privacy protection officer.

(c) Notwithstanding the provisions of subsections (a) and (b), in a database of a security authority, the details specified in section 9(b)(1A) and (3), (4), and (5) shall not be available for public review.

13. Right to Review Personal Data

(a) Every person is entitled to review, by himself or by a representative authorized by the person in writing, or by the person's guardian, the personal data held about him in a database.

(b) The database controller shall allow the review of the personal data, upon request of the person mentioned in subsection (a) (hereinafter – the requestor), in Hebrew, Arabic, or English.

(c) The database controller may refuse to provide the requestor personal data regarding the requestor's medical or mental condition if in his opinion the data may cause significant harm to the requestor's physical or mental health or risk his life; in such case, the database controller shall provide the data to a physician or a psychologist acting on behalf of the requestor.

(c1) The provisions of this section do not mandate the provision of personal data in violation of a privilege prescribed by any law, unless the requestor is the beneficiary of the privilege.

In this subsection, "law" includes case law.

(d) The manner, conditions, and fees for exercising the right to review personal data shall be determined by Regulations.

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

(1) To a database of a security authority as defined in section 19(c);

(1a) To a database of the prisons service;

(2) To a database of a tax authority as defined in the Law for the Amendment of Tax Laws (Exchange of Information between Tax Authorities), 5727-1967;

(3) Where the security or foreign relations of the state, or statutory provisions mandate not to disclose to a person data about him.

(4) To a database of entities that the Minister of Justice, in consultation with the Minister of Defense or with 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 data that state security or foreign relations mandate not to be disclosed (hereinafter – classified data), provided that a person requesting to review personal data about him and held in that database shall be entitled to review data that is not classified data;

(5) To a database of investigations and law enforcement of an authority empowered to investigate by law an offense, which the minister of justice has determined by an order, with the approval of the Constitution Committee.

(6) To a database established under section 28 of the Prohibition on Money Laundering Law, 5760-2000.

13A. Review of Personal Data Not Held by the Database Controller

Without derogating from the provisions of section 13 –

(1) A database controller, who holds the database by another (in this section – the holder), shall direct the requestor to the holder, indicating the holder's address, and instruct the holder, in writing, to allow the requestor the review;
(2) If the requestor initially approached the holder, the holder shall inform him whether he holds personal data about the requestor and the name and address of the database controller.

14. Correction of Personal Data

(a) A person who has reviewed personal data about him and found it to be incorrect, incomplete, unclear, or outdated, may request the database controller, and if he is a foreign resident – to the database holder, to correct or delete the personal data.
(b) If the database controller agrees to a request as mentioned in subsection (a), the database controller shall make the necessary amendments to the personal data in his possession and shall notify about them to anyone who received the personal data from the database controller within a period prescribed by regulations.
(c) If the database controller refused to fulfill a request as mentioned in subsection (a), he shall inform the requestor about it in the manner and form prescribed by regulations.
(d) A holder must correct personal data if the database controller agreed to the requested correction or if a court ordered the correction.

15. A Court Claim

A requestor may file a claim to the court, in the manner and form prescribed by regulations, about the refusal of a database controller to enable a review under section 13 or section 13A and about a refusal notice under section 14(c).

15A. Exemplary Damages

(a) If a database controller or a database holder violated any of the provisions specified below, a court may award, as a result of that violation, damages that do not depend on damage (in this section – exemplary damages) of up to 10,000 new shekels:

(1) Regarding a database controller – if the database is subject to registration in accordance with the provisions of section 8A – processed personal data in a database while the database was not registered, in violation of the provisions of the aforesaid section, provided that the person whose personal data relates to, demanded the registration of the database, and 90 days have passed since the day of the person's demand;

(2) Requested a person to receive personal data for the purpose of processing the personal data in a database in accordance with section 11 or 23D(a) without providing a notice as required by that section, provided that the aforesaid person demanded such notification from the controller, and 30 days have passed since the day of the person's request;

(3) Regarding a database controller – did not allow a person who requested to review personal data about him that is held in the database, to review the data, in violation of the provisions of sections 13 or 13A, within the period of time and manner prescribed by regulations in accordance with section 13;

(4) Agreed to a request to correct or delete personal data that is incorrect, incomplete, unclear, or outdated, but did not make the necessary amendments to the personal data in his possession or did not notify of the amendments to anyone who received the personal data from him within the period of time prescribed by regulations in accordance with section 14(b) in violation of the provision of that section;

(5) Did not inform the person who requested to correct or delete personal data about him, that is incorrect, incomplete, unclear, or outdated, of his refusal, in the manner and form prescribed by regulations in accordance with section 14(c), in violation of the provision of that section;

(6) Regarding a database controller – did not notify the head of the authority about the regular receipt of personal data, stored in a database in accordance with section 23D(c) provided that the person whose personal data relates to has demanded such notification from the controller, and 30 days have passed since the day of the person's request.

(b) In determining the amount of exemplary damages, the court shall consider, among others, the following specified factors, and shall not consider the extent of damage caused to the injured party as a result of the committed violation:

(1) Encouragement of the plaintiff to exercise his rights;

(2) The extent and severity of the violation;

(3) The behavior, personal circumstances, and economic capacity of the violator, as well as additional enforcement measures or payment imposed on the violator for the same violations.

(c) Nothing in this section shall derogate from the possibility to conduct a criminal proceeding if the violation also constitutes a criminal offense, derogate the possibility of using the authority under chapter D3, or derogate from the plaintiff's right to claim any other remedy in accordance with the

Torts Ordinance [New Version], for the same violation; however, a person shall not receive exemplary damages in accordance with this section more than once for the same act or omission.

16. Confidentiality

A person shall not disclose personal data obtained by him in the course of his duties as an employee, a manager, or a database holder, except for the purpose of performing his work or for implementing this law or in accordance with a court order in connection with a legal proceeding; if the motion is made before the commencement of the proceeding, the motion shall be heard in the magistrates court. Whoever violates this section shall be sentenced to 5 years imprisonment.

17. Responsibility for Data Security

(a) The database controller and the database holder are each responsible for the security of the data in the database.

(b) (1) The Minister of Justice, with the consent of the Prime Minister and the approval of the constitution committee, may prescribe regulations regarding the responsibility for data security set forth in subsection (a) and section 17B(b), including its scope and the obligations contained therein, as well as regarding the aforesaid methods of securing the data, among others, on the following matters:

(a) Physical and logical protection of the database;

(b) The management procedures and work rules in in a database and in relation to it, including the imposition of restrictions on the access of employees to the data;

(2) Regulations under paragraph (1) may establish different provisions for databases with distinct characteristics;

(3) Regulations under paragraph (1) which will apply to agencies listed in items 2 and 3 of the first schedule to the regulation of security in public bodies will be enacted also in consultation with the Minister of Defense.

17A. (Revoked)

17B. Data Security Officer

(a) The entities specified below must appoint a person with a suitable qualification to be a data security officer:

(1) A controller of five databases under a registration or a notification obligation in accordance with section 8A or a holder of five such databases;

(2) A public body as defined in section 23;

(3) A bank, an insurance company, a credit rating or evaluation company.

(b) Without derogating from the provisions of section 17, the data security officer shall be responsible for securing the data in the databases held by the entities mentioned in subsection (a).

(c) No person shall be appointed as a data security officer if the person was convicted of an offense with moral turpitude or an offense under this law.

17B1. Obligation to Appoint a Privacy Protection Officer

(a) The following entities are required to appoint a privacy protection officer:

(1) A database controller that is a public body as defined in section 23 or a database holder of such a database, excluding a security agency as defined in section 23K;

(2) A database controller whose main purpose is to collect personal data for delivering it to another as an occupation or for consideration, including direct mailing services, and the database contains personal data about more than 10,000 individuals;

(3) A database controller or a database holder whose main activities include data processing operations or involve such operations, which, given their nature, scope, or purpose, require continuous and systematic monitoring of individuals, including tracking or systematic monitoring of a person's behavior, location, or activities on a significant scale, and among others an authorized provider who provides mobile radio telephone services under the Telecommunications Law [Telecommunications and Broadcasting] 5742-1982, and a provider of an online search service or a person whose main occupation involves such actions;

(4) A database controller or a database holder whose main occupation includes processing data of special sensitivity on a significant scale, and among others a banking corporation as defined in the Banking Law (Service to Customer),5741-1981, an insurer as defined in the Supervision of Financial Services Law (Insurance), 5741-1981, a general hospital as defined in the Public Health Ordinance, 1940, and a health maintenance organization (Kupat Holim) as defined in the National Health Insurance Law, 5754-1994.

(b) For the purpose of paragraphs (3) and (4) of subsection (a) – a significant scale of data processing will be among others in consideration of the number of individuals about whom data is processed, to their proportion in a specific population, to the scope of the data, to its quantity, and to the range of types of the processed data, to the duration and frequency of the processing activities, to the duration of data retention, and to the geographic area of the processing activities.

17B2. Roles of the Privacy Officer

(a) The privacy protection officer shall act to ensure compliance with the provisions of this law by the database controller or the database holder, and to promote the protection of privacy and data security in the databases, and in this capacity will -

(1) Serve as a professional authority and a knowledge center, advise the management of the entity in which he performs his role, and its employees, prepare a training program, and supervise its implementation;

(2) Prepare a program for continuous monitoring of compliance with the provisions of this law concerning databases, ensure its implementation by the database controller or the

database holder, report his findings to the management of the entity in which he performs his role, and make suggestions to correct deficiencies;

(3) Ensure the existence of a data security procedure and the database definition document, which are required to be prepared under regulations in accordance with sections 17(b) and 36, which will be brought for approval by the management of the entity in which he performs his role;

(4) Ensure the handling of requests by individuals about whom personal data is in the database, regarding the processing of such data or the exercise of their rights under this law, including requests to review personal data or correct it; the means of contacting the privacy protection officer will be published to the public in an accessible and simple manner;

(5) Serve as the point of contact for the entity in which he performs his role, with the authority.

(b) The database controller or the database holder, as the case may be, shall provide the privacy protection officer with the conditions and resources required for the proper performance of his duties and shall ensure that the privacy protection officer is properly involved in all matters related to privacy protection laws.

(c) The privacy protection officer shall report directly to the general manager of the database controller or the database holder, as the case may be, or to an employee who reports directly to the general manager of the controller or the holder, as the case may be.

17B3. Qualifications of the Privacy Protection Officer and Fulfillment of His Role

(a) The privacy protection officer shall have the knowledge and skills required to perform his duties adequately, including in-depth knowledge of privacy protection laws, appropriate understanding of technology and data security, and familiarity with the areas of activity of the entity in which he performs his role and its objectives, taking into account the nature of the data processing, its circumstances, scope, and purposes.

(b) The privacy protection officer may be one who is not an employee of the entity in which he performs his role.

(c) The privacy protection officer shall not hold another position and shall not report to an officer of the entity in which he performs his role or in another entity, if holding the aforesaid position or subordination may place him in a conflict of interest in the performance of his duties under this law.

**Subchapter B: Direct Mailing**

17C. (Revoked)

17D. Direct Mailing

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

17E. Indication of Data Sources

A database controller or a database holder shall not process personal data in a database used for direct mailing services unless he has a record indicating the source from which each data collection used for the database was received and the date of its receipt, as well as to whom he delivered each such data collection.

17F. Deletion of Data from a Database Used for Direct Mailing

(a) Every direct mailing communication shall clearly and prominently include–

(1) An indication that the communication is a direct mailing communication, along with the indication of the registration number of the database used for direct mailing services in the database registry;

(2) A notice of the right of the recipient of the communication to be deleted from the database as mentioned in subsection (b), along with the address to which the request should be sent;

(3) The identity and address of the database controller of the database in which the personal data according to which the communication was made, is located, and the sources from which the database controller received this personal data.

(b) Any person has the right to demand, in writing, from the database controller of the database used for direct mailing services, that personal data relating to him will be deleted from the database.

(c) Any person has the right to demand, in writing, from the database controller of the database used for direct mailing services or from the database controller of the database in which the personal data according to which the communication was made, is located, that personal data relating to him will not be transferred to a person, to a type of individuals, or to specific individuals, for a limited or a permanent period.

(d) If a person notifies the database controller of his demand as mentioned in subsections (b) or (c), the database controller shall comply with the demand and notify the person, in writing, that he has acted accordingly.

(e) If the database controller does not notify as mentioned in subsection (d) within 30 days from the date of receipt of the demand, the person to whom the data relates may apply to the magistrates court in the manner prescribed by regulations for an order directing the database controller to act as stated.

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

17G. (Revoked)

17H. No Applicability to a Public Body

This subchapter does not apply to a public body as defined in section 23(1) in the performance of its duties under the law.

17I. Reservation of Laws

The provisions of this subchapter are in addition to the provisions of any law.

**Subchapter C: The Privacy Protection Authority**

17I1. The Privacy Protection Authority

(a) The head of the Authority shall supervise the compliance with the provisions of this law and its regulations regarding databases.

(b) Anyone acting on behalf of the head of the Authority is considered to be a state employee unless otherwise provided in this law.

(c) The Authority shall publish its procedures regarding the exercise of its powers on its website; however, details that constitute data that a public authority is prohibited from disclosing under section 9(a) of the freedom of information law, and the authority may choose not to publish details that constitute data that a public authority is not required 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.

17I2. Preliminary Opinion

(a) At the request of the database controller or the database holder, or the one 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 its Regulations regarding the processing of data in the database (in this law - a preliminary opinion).

(b) A request for a preliminary opinion shall include the purpose of the request and all facts necessary for the issuance of the opinion, accompanied by the relevant documents.

(c) A preliminary opinion shall be given within 60 days from the date of receipt of the said request in subsection (b) or from the date on which the relevant documents are provided, whichever is later; the head of the authority may extend the date, under special circumstances; if the authority decides not to issue a preliminary opinion, it will notify the requester within 45 days from the said date.

(d) The authority may publish a preliminary opinion with the consent of the requester; if the requester does not consent to the publication of the preliminary opinion, the Authority may publish it without identifying details.

(e) The head of the authority shall determine a procedure, which shall be published on the authority's website, regarding how to submit a request for a preliminary opinion and circumstances in which an opinion will not be given for requests of the following types:

(1) A request for which the authority's position has already been published in the past or for which there is a clear precedent;

(2) A request whose scope and implications are limited to the requester's matter relative to the considerable allocation of resources that its handling will require;

(3) A request that is theoretical or academic in nature;

(4) A request tainted by lack of integrity;

(5) A request relating to pending proceedings, including supervision, inquiry, or criminal enforcement procedures, in accordance with this law;

(6) A request whose handling will require an unreasonable allocation of resources.

17I3. Report on the Activities of the Privacy Protection Authority and Reporting to the Constitution Committee

(a) 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 the enforcement and supervision actions (in this section - the 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 each year, to the constitution committee.

(b) The report on the activities of the privacy protection authority shall include, among other things, information detailed as follows, categorized according to government ministries, other public bodies, and private entities:

(1) The number of requests for preliminary opinions submitted to the authority and the number of opinions issued;

(2) The number of requests for database registration 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 the refusal or suspension;

(3) The number of databases required to be registered under section 8a(a) that were exempted from the registration requirement;

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

(5) The number of notices about databases submitted to the privacy protection authority under section 8a(b) and the number of controllers or holders of the said databases, that supervision or administrative inquiry were conducted against, in the year following the submission of the notification;

(6) The number of complaints submitted to the authority against controllers or holders of databases regarding violations under this law;

(7) The number of sectoral supervisions conducted under section 23IZ;

(8) The number of administrative inquiry procedures initiated under section 23JB(a), and for how many of them it was decided to conduct an investigation instead of an inquiry procedure, under section 23IG(b);

(9) The number of search and seizure warrants, or computer material access warrants requested from the court under section 23JD(a) and the number of cases in which the warrant was granted;

(10) The number of complaints submitted to the head of the authority about an external expert under section 23JH(h), and how many of them were found to be justified;

(11) The number of orders to cease violations issued under section 23KE, categorized by types of violations, how many appeals regarding the orders were filed, and how many appeals were fully or partially accepted;

(12) The number of administrative alerts issued under section 23LF, and for how many of them a cancellation request was submitted under section 23LG, and what were the outcomes of the request;

(13) The number of cases in which the violator was notified of the possibility of submitting a letter of undertaking and deposit a surety bond instead of imposing a monetary sanction under section 23LI, and in how many cases the violator submitted a letter of undertaking and deposited a surety bond under section 23M(c);

(14) The total monetary sanctions imposed under section 23KF, the average imposed monetary sanction amount, the highest monetary sanction imposed, and the lowest monetary sanction imposed;

(15) The number of cases in which a violator sought to exercise the right to be heard under section 23KH, and the average time taken to exercise the right to be heard;

(16) The number of cases in which a monetary sanctions notice was issued, and no monetary sanction was imposed, and the reasons for non-imposition;

(17) The number of cases in which the monetary sanction was reduced under section 23la and schedule 5, in how many of them the sanction was reduced because it exceeded the maximum permissible rate from the entity's turnover, in how many of them - because it exceeded the cap for a small or micro enterprise under the same schedule, and in how many of them - because a privacy officer was appointed in the entities listed in section 17b1(a)(3) and-(4);

(18) The number of repeated violations that occurred, how many of them occurred after an administrative warning in accordance with section 23LF, and how many occurred after submitting a letter of undertaking and depositing a surety bond under section 23M;

(19) The number of repeated violations that occurred;

(20) The number of appeals filed against the head of the authority's decisions to impose a monetary sanction, administrative alert, or a letter of undertaking and a surety bond under chapter D'3, in how many of them the execution of the decision was delayed, and in how many of them the appeal has been accepted;

(21) The number of cases in which a monetary sanction imposed on a corporation was not published, and the number of cases in which a monetary sanction imposed on an individual or corporation was published as stated in section 23MF;

(22) The number of requests submitted for a cessation order under section 23MI, and in how many of them the said order was granted;

(23) Data on the criminal enforcement carried out by the authority, and among others the number of investigations initiated by an investigator, the number of indictments filed following the said investigations, categorized according to offense sections, and in how many of them the proceedings ended in conviction, and what were the penalties in each case;

(24) The number of requests submitted to approve the exercise of powers by the head of the Authority, inspector, or investigator submitted to the chairman of the central election committee or the chairman of the regional election committee, as the case may be, in accordance with section 23NI; how many of them were accepted, and in how many of them conditions were set.

(c) To report on the activities of the privacy protection authority under subsection (a) the head of the authority shall include a report on the number of lawsuits filed in court for compensation without proof of damage under section 15a and the case numbers of the said lawsuits, according to the information provided to him by the court administration.

## CHAPTER C: Defenses

18. What are Defenses

In a criminal, civil, or administrative trial due to a privacy invasion, it will be a good defense if one of the following applies:

(1) The invasion was made through a publication protected under section 13 of the Prohibition of Defamation Law, 5725 – 1965;

(2) The defendant or accused acted in good faith under one of these circumstances:

(a) He did not know and could not have known about the potential invasion of privacy;

(b) The invasion occurred under circumstances where the invader had a legal, moral, social, or professional obligation to commit it;

(c) The invasion was done to protect a legitimate personal interest of the violator;

(d) The invasion occurred as part of the invader's lawful occupation and during his regular course of work, provided that it was not done through publication to the public;

(e) The invasion occurred through photography or publication of a photograph taken in a public place, where the injured party’s image appeared incidentally;

(f) The invasion was made through a publication protected under paragraphs (4) to (11) of section 15 of the Prohibition of Defamation Law, 5725 – 1965

(3) There was a public interest in the invasion justifying it under the circumstances, provided that if the invasion was through publication – it was not false.

19. Exemption

(a) A person will not be liable under this law for an act he was authorized to do according to the law.

(b) A security authority or anyone acting on its behalf will not be liable under this law for an invasion committed reasonably within their role and for fulfilling it.

(c) "security authority" in this section means:

(1) Israeli Police;

(2) Intelligence Directorate of

the General Staff and the Military Police of the Israeli-Defense Forces;

(3) the Israeli Security Agency (Shin Bet);

(4) the Institute for Intelligence and Special Operations (Mossad);

(5) The Witness Protection Authority.

20. Burden of Proof

(a) If the defendant or accused proves that he committed the privacy invasion under one of the said circumstances in section 18(2) and that the invasion did not exceed the reasonable limits under those circumstances, it will be presumed that the invasion was done in good faith.

(b) It will be presumed that the defendant or the accused did not commit the invasion in good faith if he knowingly caused more harm than was reasonably necessary for the protected matters under section 18(2).

(c) It will be presumed that the defendant or accused did not commit the invasion in good faith, if he executed the invasion while violating ethical rules or principles applicable to his profession by law or by those accepted by the professionals of the field to which he belongs; however, this presumption will not apply if the invasion occurred under circumstances where the defendant or accused acted according to a legal obligation imposed on him.

21. Rebuttal of Defense Claims

If the defendant or accused presents evidence or testifies to establish one of the defenses provided by this law, the plaintiff may present contradictory evidence; this provision does not detract from the court's authority under any law to allow the presentation of evidence by the litigants.

22. Mitigating Factors

When sentencing or awarding damages, the court may also consider the following in favor of the defendant or accused:

(1) The privacy invasion was merely a repetition of what had already been said, and he cited the source on which he relied;

(2) He did not intend to invade;

(3) If the invasion was through publication – he apologized for the publication and took steps to stop the sale or distribution of the publication copy containing the invasion, provided the apology was published in the same place, manner and extent, as the invasion and was not qualified.

**CHAPTER D: Providing Information or Data by Public Bodies**

23. Definitions

In this chapter

"Public Body" means:

(1) Government ministries and other state institutions, local authorities, and another body performing public functions in accordance with the law;

(2) A body designated by the minister of justice by order, with the approval of the constitution committee, provided that the order specifies the types of information and data the body is authorized to provide and receive.

23A (revoked)

23B. Prohibition on Providing Data

(a) Providing personal data by a public body is prohibited unless the data was lawfully published to the public or made available for the public's review by legal authority, or the person to whom the personal data relates, has consented to its provision.

(b) The provisions of this section do not prevent a security authority, as defined in section 19, from receiving or providing personal data for fulfilling its role, provided that the provision or receipt is not prohibited by law.

23C. Exception to the Prohibition

The provision of personal data is allowed, despite the said in section 23B, if not prohibited by law or professional ethics principles–

(1) Between public bodies, if one of the following applies:

(a) The provision of personal data is within the powers or obligations of the data provider and is necessary for the purpose of implementing a law or for the purpose within the powers or obligations of the provider or recipient;

(b) The provision of personal data is to a public body authorized to request the same data by law from any other source;

(2) From a public body to a government ministry or another state institution, or between the said ministries or institutions, if the provision of personal data is necessary for the purpose of implementing any law or for the purpose within the powers or obligation of the provider or recipient;

However, personal data given under the condition that it will not be provided to another shall not be provided.

23D. Obligations of a Public Body

(a) A public body that regularly provides personal data under section 23C must specify this fact on any data request under the law.

(b) A public body providing personal data under section 23C must keep a record of the personal data provided.

(c) A public body that regularly receives personal data under section 23C, and the personal data is stored in a database, will notify the head of the authority, and this fact will be included in the details of the database registry under section 12.

(d) A public body that received personal data under section 23C must not use it except within the frame of its powers or obligations.

(e) Regarding the confidentiality obligation under any law, personal data provided to a public body under this law is equivalent to personal data the body obtained from any other source, and in addition, the receiving body will also be subject to all provisions applicable to the providing body.

23E. Excessive Personal Data

(a) Where the personal data permitted to be provided under sections 23B or 23C is contained on the same file with other personal data (hereinafter – excessive personal data), the providing body may provide to the receiving body the personal data with the excessive personal data.

(b) The provision of excessive personal data under subsection (a) is conditioned with the establishment of procedures guaranteeing the prevention of any use of the received excessive personal data; such procedures will be established in Regulations, and until established in Regulations, the requesting body will establish such procedures in writing and provide the providing body with a copy upon request.

23F. Permitted Provision Does Not Invade Privacy

Providing personal data permitted by this law will not constitute a privacy invasion, and sections 2 and 8 will not apply.

23G. Regulations on The Provision of Personal Data

The Minister of Justice, with the approval of the constitution committee, may enact Regulations regarding the procedures for providing personal data by public bodies.

23H. (Revoked)

## CHAPTER D1: Supervisory and Administrative Inquiry Powers

### Subchapter A: Appointment of Inspectors

23I. Appointment of Inspectors

(a) The head of the authority may appoint an inspector from among state employees, who will have all or some of the powers under this law, if all the following apply to him:

(1) The Israeli police has notified, within three months of the head of the authority's request, that it does not object to his appointment for reasons of public safety, including due to his criminal record;

(2) He received appropriate training in the domain of the powers he will have under this law and met additional qualification conditions, if prescribed, as instructed by the Minister of Justice, with the agreement of the Minister of National Security, and regarding the exercise of powers to the access or copy of computer material as stated in section 23JD – he holds a position qualified to perform such activities;

(3) He received appropriate training in privacy protection, as instructed by the Minister of Justice.

(b) The inspector's authorization under this section will be on a certificate signed by the head of the authority, certifying his role as an inspector and his powers under this law (hereinafter – inspector's certificate).

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

### Subchapter B: Supervisory Powers

23J. Inspector's Powers

(a) To supervise the implementation of the provisions under chapters B, D, and E, and to supervise the implementation of the instructions that the head of the authority is authorized to instruct their violation cessation in accordance with section 23KH, an inspector appointed under the provisions of subchapter A (hereinafter – inspector) may:

(1) Require any person he believes to be involved in the matter to provide his name and address and present an identity document or other official identification document;

(2) Require any involved person to provide any information or document;

(3) Require any involved person to present or provide a copy of computer material containing system data or sample data; sample data under this section will not be collected in a manner more extensive than necessary to achieve the supervisory purposes;

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

(b) Prior to exercising his powers under this section, the inspector will notify the person that he is under supervision procedure; once notified as said, the person must answer the questions he is asked, but the answers will not be used as evidence in a criminal proceeding against him, if he had no obligation to answer them if asked under section 2(2) of the Criminal Procedure Ordinance (Testimony).

(c) The head of the authority will delete system data or sample data provided or collected under subsection (a)(3) when they are no longer reasonably required for continuous supervisory procedures, and no later than three years from the data provision or collection date, and regarding system data – within seven years unless the data is required for proceedings under subchapter B or C of this chapter, under chapter D'3, or under chapter D'4.

23JA. Inspector Identification

An inspector will not exercise the powers granted to him under this chapter, except while performing his role and if both of the following apply:

(1) He openly wears a badge identifying him and his role;

(2) He has an inspector's certificate, which he will present upon request.

**Subchapter C: Administrative Inquiry**

23JB. Administrative Inquiry

(a) If an inspector has reasonable grounds to assume that a violation of a provision out of the instructions that the head of the authority is authorized to order the cessation of under section 23KE, or a provision under this law as mentioned in section 23KF, he may initiate an administrative inquiry procedure regarding the violation and exercise the powers under section 23J.

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

(1) thwart the exercise of power by the inspector;

(2) Endanger the inspector's or another person's safety.

(c) If the reason for which the inspector did not fulfill the identification requirement as mentioned in subsection (b) has passed, the inspector will fulfill the said obligation as soon as possible.

23JC. Notice of Administrative Inquiry Procedure and Response to Inspector's Questions

Before exercising his powers under this subchapter, the inspector will notify the person that an administrative inquiry procedure concerning the database is being conducted and the nature of the inquiry; once notified as mentioned, the person must answer the questions asked, but the answers will not be used against him as evidence in a criminal proceeding if he would not have been required to answer them if asked under section 2(2) of the Criminal Procedure Ordinance (Testimony).

23JD. Search and Seizure Order and Warrant for Access to Computer Material

(a) If an inspector that the head of the authority has appointed to do so, has reasonable grounds to believe that a violation of a provision under this law as mentioned in section 23JB(a) has been committed, he may request a search and seizure order or an order for access to computer material under sections 23(1), 23A, and 24 of the Arrest and Search Ordinance, and execute it himself or through another inspector; notice of an authorization under this subsection will be published in the Official Gazette.

(b) Data collected through access to computer material during an administrative inquiry procedure will be used solely for the purpose for which it was collected, and will not be used as evidence in a criminal proceeding.

23IF. Way of Conducting a Search, Seizure of an Object, and Access to Computer Material and Its Copying

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 will apply when conducting a search, seizure of an object, and access to or copying of computer material under this subchapter, with the necessary modifications, and these changes: the powers granted to a police officer will be given to the inspector, and the powers granted to a police sub-Inspector will be given to the head of the authority or an inspector appointed by the head of the authority.

23IG. Decision on Administrative Inquiry Procedure in Case of Reasonable Suspicion of Criminal Offense

(a) If the head of the authority has reasonable grounds to suspect that an act or omission (in this chapter – act) that justifies a criminal investigation under subchapter A of chapter D'4 or an administrative inquiry under this subchapter, the head of the authority will determine on conducting an investigation or administrative inquiry; the head of the authority's determination will be based solely on these considerations and according to an enforcement procedure determined by the head of the authority:

(1) the severity of the act and its circumstances;

(2) the assessment of the nature and strength of the evidence related to the same act;

(3) The enforcement policy of the authority.

(b) If the head of the authority decides to conduct an administrative inquiry procedure under subsection (a) and new facts that were unknown to the authority and if known would have influenced the decision are discovered, the head of the authority may order an investigation instead of the inquiry procedure.

(c) The head of the authority may delegate his power under subsection (a), to decide to conduct a criminal investigation or administrative inquiry to a senior employee who reports directly to him; notice of such delegation will be published in the Official Gazette.

**Subchapter D: Sectoral Supervision and External Experts**

23JG. A Plan for Sectoral Supervision and Assistance from Non-civil Servants for Sectoral Supervision

(a) The head of the authority shall determine a plan for sectoral supervision of the implementation of provisions under this law and a list of supervised entities to which the sectoral supervision plan shall 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 – assisting agent):

(1) Distributing the sectoral supervision questionnaires to the supervised entities, provided that it is clarified that the request to the supervised entity is on behalf of the authority, but that the response and communication shall be conducted with a non-civil servant and that the supervised entity shall be entitled to contact the civil servant whose name and details shall be indicated in the request;

(2) Receiving of the response to the questionnaire from the supervised entity, including the requested accompanying documents and any additional documents attached by the supervised entity;

(3) Examination of the response to the questionnaire and the documents received in accordance with paragraph (2), in accordance with the criteria to be determined by the head of the authority in a procedure;

(4) Contacting the supervised entity for supplementary information or to update it on the need to clarify the answers with the authority;

(5) preparation of a report to the authority regarding the supervised entity's response to the questionnaire for a specific supervised entity or type of supervised entities;

(6) Granting an extension requested by a supervised entity for a response to the questionnaire or submission of documents according to the authority's guidelines;

(7) Providing technical answers to the supervised entity.

(b) In performing the actions, the assisting agent shall act under the direction and instructions of the head of the authority and under his supervision; however–

(1) Any action requiring the exercise of discretion granted to the authority or its employees by law shall only be performed by a civil servant;

(2) An assisting agent shall not perform an action requiring entry to a place under the provision of section 23J(a)(4).

(c) The provisions of section 23JH(c)(2) to (e), (g), (j) and (ja) shall apply to an assisting agent, with the required changes.

23JH. Assistance from an External Expert

(a) In order to supervise the fulfillment of the provisions under chapters B, D, and E and to exercise his powers under subchapters B and-C, and chapter D'3, the head of the authority may be assisted by a person who is non-civil servant, and who has been granted authorization according to the provisions of subsection (c) (in this law — an expert external), in matters for which experience, knowledge or unique means are required.

(b) An external expert shall act on behalf of the head of the authority, under his directions and instructions and under his supervision; the external expert shall not exercise a power involving the exercise of discretion granted to the head of the authority or to employees of the authority by law.

(c) The head of the authority may grant authorization to serve as an external expert to a person who meets all the following:

(1) He has the experience, knowledge and expertise appropriate to his position;

(2) 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.

(d) The head of the authority may refuse authorization to serve as an external expert to a person 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) (1) No one shall be appointed to serve as an external expert or continue in this role if his position shall frequently place him in a conflict of interest;

(2) An external expert shall not handle a matter that shall place him in a conflict of interest;

(3) If an external expert becomes aware that he may be placed in a conflict of interest as mentioned 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 accompany an inspector entering the premises in accordance with the provisions of section 23J(a)(4).

(g) An external expert who receives data according to this section during the fulfillment of his duty or work must keep it confidential, not disclose it to another, and not use it except in accordance with this law or other legislation or by a court order.

(h) Anyone that sees himself injured by the action of an external expert may file a detailed written complaint to the head of the authority; the head of the authority shall examine the complaint and respond to the applicant within 45 days; if the head of the authority finds the complaint justified, he shall notify the applicant and the external expert, along with his decision; if the head of the authority finds the complaint unjustified, he shall inform the applicant and the external expert in writing.

(i) (1) The external expert is subject to the same legal provisions as civil servants regarding public servant laws in the Penal Code, 5737-1977, and the Public Service (Gifts) Law, 5749-1979;

(2) Restrictions on the external expert's activities after the termination of the engagement with him shall be determined in the contract, including provisions regarding the period in which the external expert shall not work for a competitor of the entity he dealt with as an external expert, nor provide services or receive benefits from such an entity.

(j) A notice of authorization to serve as an external expert and an updated list of external experts shall be published on the authority's website.

(k) In this section—

"family member" – spouse, parent, grandparent, son or daughter and their spouses, sibling and their children, mother-in-law, grandson or granddaughter, including a relative as mentioned that is intertwined (step);

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

"handling" – including making decisions, raising a subject for discussion, presence in a discussion, participation in a discussion or vote, or dealing with the subject outside the discussion;

"conflict of interest" of an external expert – a conflict of interest between the fulfillment of his duties and a personal interest or other position, his own or that of his relative;

"relative" – any of the following:

(1) a family member of an external expert;

(2) a person in whom an external expert has an interest in his financial situation;

(3) a corporation in which an external expert, his family member or a person referred to in paragraph (2) has an interest;

(4) An entity in which an external expert, his family member or a person referred to in paragraph (2) are responsible managers or employees.

**Subchapter E: Supervision and Administrative Inquiries in Bodies Under the Regulation of Security in Public Bodies**

23JI. Supervision and Administrative Inquiry in Bodies Listed in the fifth schedule to the Public Security Regulation Law.

The manner of exercising the powers in accordance with subsections B and C regarding the bodies listed in schedule 5 to the Public Security Regulation Law, shall be determined in a procedure formulated in agreement between the National Cyber Directorate as defined in the aforementioned law (in this law – the National Cyber Directorate) and the authority, considering the sensitivity of the data and computerized systems used by these bodies.

**CHAPTER D2: Supervision and Administrative Inquiry in Security Agencies**

23K. Applicability to Security Agencies

(a) In this chapter—

"security agency" – one of the following:

(1) the Israeli Police;

(2) the Israel Defense Forces;

(3) the Israel Security Agency (Shin Bet);

(4) the Institute for Intelligence and Special Operations (Mossad);

(5) the National Cyber Directorate;

(6) the Witness Protection Authority;

(7) the Israel Prison Service;

(8) the Ministry of Defense and its auxiliary units and the Director of Security in the Defense Establishment;

(9) units and auxiliary units of the Prime Minister's Office, whose main activity is in the domain of national security;

(10) enterprises included in an order issued by the Minister of Defense pursuant to item (3) of the first schedule to the Public Security Regulation Law, and which the Minister of Defense notified the Minister of Justice;

(11) 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", for the purposes of the Israel Defense Forces – the Chief of the General Staff or an officer with the rank of Major General authorized by the Chief of the General Staff for this purpose.

(b) (1) The provisions of subchapters B and C of chapter D'1 shall not apply to security agencies, but the supervision and administrative inquiry of security agencies shall be carried out in accordance with the provisions of this chapter;

(2) Notwithstanding the provisions of paragraph (1), the Israeli Police shall be subject to the provisions of subchapters B and C of chapter D'1, provided that they do not apply to databases classified as "secret" or higher.

(c) The Minister of Defense, with the consent of the Minister of Justice, may not include in the publication in the Official Gazette of an order as stated in paragraph (11) of the definition "security agency" in subsection (a), the name of an agency in respect of which the said order was issued, for reasons of protecting national security; however, the full text of the order, which includes the name of said agency, shall be deposited with the Minister of Justice.

23KA. Appointment of a Privacy Inspector in a Security Agency

(a) The head of a security agency, in consultation with the head of the authority, shall appoint a person to the position of a privacy inspector in the security agency (in this chapter – the internal inspector), according to the qualifications and training terms instructed by the head of the authority, in consultation with the head of the security agency.

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

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

(d) The internal inspector shall be an employee of the security agency which will report directly to the head of the security agency, or to a senior employee of the security agency who directly report to the head of the security agency and shall be professionally instructed by the head of the authority.

(e) The internal inspector shall not perform any additional position or engage in any additional occupation that may place him in concern of a conflict of interest in the performance of his duties under this chapter.

(f) The security agency shall make available to the internal inspector appropriate means necessary to fulfill its duties under this chapter.

23KB. Duties of the Internal Inspector

The internal inspector shall supervise the implementation of the provisions of this law in the security agency and shall supervise their implementation, among others:

(1) Prepare an annual work plan to be submitted for approval by the head of the security agency and the head of the authority, to supervise compliance with the provisions of this law and to examine violations of provisions that the head of the authority is authorized to order to cease violating under section23KE and violation of any of the provisions under this law detailed in section 23KF (in this section – work plan);

(2) examine the procedures of the security agency and its policy in the domain of privacy protection and its compliance with the provisions of the law and the security agency's policy in the domain of privacy protection and its compliance with the provisions under this law;

(3) examine the existence of violations of provisions which the head of the authority is authorized to order to cease violating under section 23KE and violation of the provisions under this law detailed in section23KF, in accordance with the instructions of the head of the authority;

(4) Report to the head of the authority without delay, subject to the security adjustment provisions, within the meaning of section 15 of the Israel Security Agency Law, 5762-2002, and the classification applicable to the security agency, on the findings of the supervision and examination activities it has conducted;

(5) Supervise the manner in which deficiencies discovered in the findings of the supervision and examination are corrected;

(6) Conduct training and instruction to the employees of the security agency on privacy issues;

(7) Submit to the head of the security agency and to the head of the authority an annual report on the manner in which the work plan is implemented and on compliance with the provisions of the law in the domain of privacy protection in the security agency.

23KC. Powers of the Internal Inspector

In order to fulfill his duties, the internal inspector shall have the powers given to the inspector under subchapter B of chapter D'1, and shall also be obligated to delete sample data as provided in section 23J(c), with the necessary changes.

23KD. Powers of the Head of the Authority regarding Security Agencies

(a) The head of the authority may instruct the internal inspector to take actions, including complementary or additional actions to those conducted by the internal inspector, or to act to correct deficiencies.

(b) The head of the authority may exercise the powers delegated to him under chapter D3 if he finds that any of the instructions that the head of the authority is authorized to order the cessation of its

violation according to section 23KE, or a provision detailed in section 23KF has been violated, on the basis of a report by the internal inspector, or if he finds that there is a concern that any of the provisions detailed as aforesaid have been violated, and instructed the internal inspector to ascertain whether a violation has been committed, and the internal inspector did not investigate the violation within a reasonable time determined by the head of the authority after consulting with the internal inspector, and the provisions of section 23KG have been complied with.

(c) If the head of the authority believes that the findings stated in subsection (a) or (b) raise suspicion that an offense has been committed under this law, or that he has otherwise become aware of the commission of such an offense, the investigator shall have the enforcement powers under section 23NA, unless there was another investigative authority authorized by law to investigate offenses in that security agency; for the purposes of this section, "other investigative authority" – other than the Israeli Police.

(d) An investigator or the head of the authority shall not use his powers under this chapter against a security agency unless he has undergone security adjustment within the meaning of section 15 of the Israel Security Agency Law, 5762-2002.

**CHAPTER D'3: Administrative Enforcement Measures and Judicial Order**

**Subchapter A: The Power of the Head of the Authority to order the Cessation of a Violation**

23KE. Power to order the Cessation of a Violation

(a) If the head of the authority finds that a database controller or a database holder has used knowledge of a person's private affairs in a database other than for the purpose for which it was provided, contrary to the provisions of section 2(9), or processed personal data in a database for a purpose that constitutes an invasion 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 instruct him to cease it in the manner and within a period determined.

(b) If the head of the authority finds that a database controller or a database holder has processed personal data in a database created, received, accumulated or collected, contrary to the provisions of this law or contrary to the provisions of any other law regulating data processing, or has permitted another to process such personal data for him, contrary to section 8(d), he may, after giving him an opportunity to argue his claims, notify him that his actions constitute a violation and instruct him to cease it in the manner and within a period as determined.

(c) If the head of the authority finds that a database controller or a database holder has processed data contrary to the provisions of the regulations detailed in part B of schedule 4, he may, after giving him an opportunity to present his arguments, notify him that his actions constitute a violation and instruct him to cease it in the manner and within a period as he may direct.

(d) If the head of the authority finds that the provisions of paragraphs (1) to (4) below have been complied with, he may, after giving the database controller or the database holder who is required to appoint a privacy protection officer in accordance with section 17B1(a), an opportunity to present his arguments, notify him that his actions constitute a violation, and instruct him to cease the violation and the manner in which it should be rectified; if the minister of justice determines, with the approval of the constitution committee, an order under section 23KF(d)(1)(g), the head of the authority may also issue such an order for the purposes of paragraph (5) below:

(1) the privacy protection officer has not been provided with the necessary conditions and resources for proper performance of his duties, or he was not adequately involved in all matters related to privacy protection laws, contrary to section 17B2(b);

(2) the privacy protection officer does not report directly to the officials listed in section 17B2(c);

(3) the privacy protection officer does not possess the required knowledge and skills according to section 17B3(a);

(4) the privacy protection officer holds another position or reports to an official in the entity where he serves or in another organization, which may cause a conflict of interest in fulfilling his duties under this law, contrary to section 17B3(c);

(5) the database controller or the database holder did not appoint a privacy protection officer, contrary to section 17B1(a)(3) or (4).

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

(1) details of the act or omission (in this chapter – the act) that constitutes the violation, the circumstances of its commission and the date of its commission, the requirement to rectify the violation and the date for its rectification;

(2) the possibility of imposing a financial sanction on the violator if he does not cease the violation;

(3) the violator's right to appeal within 45 days according to paragraph (f).

(f) (1) an order by the head of the authority to cease a violation can be appealed to the magistrate's court where the president of the magistrate's court presides, within 45 days from the day the notice of the cessation of the aforesaid violation was delivered;

(2) 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 may return the matter with instructions to the head of the authority;

(3) if an appeal is filed as detailed, the violation of the head of the authority's order under this section shall not be considered a violation until the court issues another order.

(g) The head of the authority may delegate his powers under subsections (a) to (c) to a senior employee directly reporting to him; a notice of such delegation shall be published in the official gazette.

**Subchapter B: Imposition of Monetary Sanctions**

23KF. Monetary Sanctions

(a) If a database controller or a database holder violates any of the provisions under this law, as specified below, the head of the authority may impose a monetary sanction on him in the amount of 150,000 new shekels, and if the database contained personal data about 1,000,000 individuals or more, the head of the authority may impose double the amount on him:

(1) Committed one of the following:

(a) processed personal data in a database required to be registered without it being registered, contrary to the provisions of section 8A(a);

(b) included incorrect details in an application for registration of a database submitted under section 9, contrary to the provisions of that section;

(c) did not notify the head of the authority of a change in the details listed in section 9(b) or in the details determined pursuant to section 9(c), contrary to the provisions of section 9(d), except for a change in the address of the database controller;

(2) fails to provide the head of the authority with notice of a database that is required to be notified under section 8A(b) or fails to notify the head of the authority of a change in any of the details specified in that section, contrary to the provisions of that section;

(3) processed personal data 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, contrary to the provisions of section 17D;

(4) Fails to inform the head of the authority that he regularly receives personal data in accordance with the provisions of section 23C and the data is stored in a database, contrary to the provisions of section 23D(c).

(b) If a database controller or a database holder violates any of the provisions of this law, as specified below, the head of the authority may impose a monetary sanction on him under the provisions of this chapter, in the amount of 15,000 new shekels:

(1) refused to allow a person about whom personal data is held in the database to review the personal data about him, contrary to the provisions under section 13;

(2) made a change to the personal data in his possession without notifying all those who received the data, contrary to the instructions under section 14(b);

(3) fails to notify the applicant of a refusal to correct personal data held in a database in his possession or delete it, contrary to the provisions under section 14(c);

(4) did not correct personal data held in a database in his possession, contrary to the provisions of section 14(d);

(5) does not comply with a person's request pursuant to section 17F(b) that personal data relating to him be deleted from a database used for direct mailing, contrary to the provisions of section 17F(d);

(6) fails to comply with a person's request pursuant to section 17F(c) that personal data relating to him not be disclosed to a person, type of individuals or specific individuals, contrary to the provisions of section 17F(d).

(c) (1) If a database controller or a database holder violates any of the provisions of this law, as specified below, the head of the authority may impose a monetary sanction on him under the provisions of this chapter, in the amount of 50 new shekels multiplied by the number of individuals to whom the inquiry or request was made, as specified below, and if the inquiry or request related to data of special sensitivity – in the amount of 100 new shekels multiplied by the number of individuals as aforesaid:

(a) contacted a person for the provision of personal data for processing in a database, without providing him notice as required by section 11;

(b) contact a person by direct mailing, contrary to the provisions of section 17F(a);

(c) a database controller who has not specified the requirement of personal data, that he regularly provides data in accordance with section 23C, contrary to the provisions of section 23D(a);

(2) If the amount of the monetary sanction under paragraph (1) is less than 30,000 new shekels, the head of the authority may impose a monetary sanction in the amount of 30,000 new shekels on a database controller or database holder.

(d) (1) If a database controller or a database holder violates any of the provisions of this law, as specified below, the head of the authority may impose a monetary sanction on him under the provisions of this chapter in the amount of 2 new shekels for each person about whom personal data is held in the database, and if the personal data in the database was data of special sensitivity – in the amount of 4 new shekels per person:

(a) contacted a person for the provision of personal data for processing in a database, and the inquiry was made to an unspecified group of individuals, without providing him notice as required by section 11, contrary to the provisions of the said section;

(b) did not appoint a data security officer, contrary to the provisions of section 17B(a);

(c) did not appoint a privacy protection officer, contrary to the provisions of section 17B1(a)(1) or (2);

(d) processed personal data in a database used for direct mailing services, without maintaining a record indicating the source from which he received each data collection used for the purpose of the database and the date it was received, as well as a record indicating to whom each such data collection was provided, contrary to the provisions of section 17E;

(e) a database controller that does not maintain a record of the personal data provided by him in accordance with section 23C, contrary to the provisions of section 23D(b);

(f) with regard to a database controller listed in section 17B1(a)(1) or (2) – did not comply with the instructions of the head of the authority to cease or correct a violation, contrary to the provisions of section 23KE(d);

(g) The Minister of Justice, with the approval of the constitution committee, may determine, by order, that the provisions of subparagraph (f) shall also apply to the database controller or the database holder listed in section 17B1(a)(3) and (4);

(2) In a monetary sanction under subparagraphs (d) and (e), the amount of the monetary sanction shall be calculated based on the number of individuals about whom there is no record as stated in those subparagraphs;

(3) If the amount of the monetary sanction under paragraph (1) is less than 20,000 new shekels, and if the personal data in the database was data of special sensitivity – less than 40,000 new shekels, the head of the authority may impose a monetary sanction on a database controller or database holder in the amount of 20,000 new shekels or 40,000 new shekels, as applicable.

(e) (1) If a database controller or a database holder violates any of the provisions under this law, as specified below, the head of the authority may impose a monetary sanction on him under the provisions of this chapter in the amount of 4 new shekels for each person to whom personal data is held in the database, and if the personal data in the database was data of special sensitivity – in the amount of 8 new shekels per person:

(a) fails to comply with the instructions of the head of the authority under section 23KE(a) to cease using data about a person's private affairs in a database other than for the purpose for which it was provided, contrary to the provisions of section 2(9), or to cease processing personal data in a database for a purpose that constitutes an invasion of privacy under section 2;

(b) processed personal data in a database for an unlawful purpose, contrary to the provisions of section 8(b), unless the processing was only contrary to the provisions of section 2;

(c) fails to comply with the instructions of the head of the authority in accordance with section 23KE(b) to cease processing personal data in a database created, received, accumulated or collected, contrary to the provisions of this law or contrary to the provisions of any other law regulating data processing, or to cease allowing another to process such personal data on his behalf;

(d) processed personal data without the authorization of the database controller, or in excess of the said authorization, contrary to the provisions of section 8(c);

(e) a database controller who provided data from a public body, contrary to the provisions of section 23B, without complying with the provisions of section 23C;

(2) If the amount of the monetary sanction provided in paragraph (1) is less than 200,000 new shekels, the head of the authority may impose a monetary sanction in the amount of 200,000 new shekels on a database controller or database holder.

(f) If a database controller or a database holder processed personal data in a database other than in accordance with the purpose that was specified, contrary to the provisions of section 8(b), in circumstances where such a purpose could have been lawfully determined, the head of the authority may impose a monetary sanction on him according to the provisions of this chapter in the amount specified in detail (1) of schedule 3.

(g) If a database controller or a database holder fails to provide a document or copy of computer material to the inspector, contrary to the provisions of section 23J(a)(2) or (3), the head of the authority may impose a monetary sanction on him under the provisions of this chapter in the amount of 300,000 new shekels.

(h) If a database controller or a database holder violates any of the provisions of the regulations established pursuant to section 36, as specified in column A of schedule 3, which applicable to him, the head of the authority may impose a monetary sanction on him under the provisions of this

chapter in the amount specified in relation to him in column B, column C, column D, or column E alongside that provision, as the case may be, and if the database is a database to which the high level of security applies in the aforementioned schedule and contains data about 1,000,000 individuals or more, the head of the authority may impose double the amount set forth in column E next to that provision.

(i) (1) If a database controller or a database holder violates any of the provisions of the regulations established under section 36 of schedule 4, as specified in column A of part A of that schedule, the head of the authority may impose a monetary sanction on him under the provisions of this chapter in the amount specified in column B alongside that provision;

(2) If a database controller or a database holder of another database did not comply with the instructions of the head of the authority pursuant to section 23KE(c) to cease violating the provisions of the regulations as stated in part B of schedule 4, the head of the authority may impose a monetary sanction on him under the provisions of this chapter, in the amount specified in column B alongside that provision in that schedule.

(j) (1) If the database holder is provided with a demand for payment due to a violation of a provision as stated in subsection (h), the head of the authority shall notify the database controller along with a copy of the payment demand given to the database holder, and instruct the database controller to cease the violation by the database holder, all within a period, as directed by the head of the authority;

(2) If the violation as stated in paragraph (1) was not ceased, and the database controller did not comply with the head of the authority's instructions to him to cease the violation, the head of the authority may issue him a notice of intended charge as stated in section 23KG due to that violation, and the provisions under this subchapter shall apply to the database controller regarding that violation, with necessary adjustments, as if he were the violator; the amount of the monetary sanction imposed on the database controller due to such a violation shall be the amount that can be imposed on the database holder for that violation.

23KG. Notice of Intended Charge

(a) If the head of the authority has reasonable grounds to believe that a person has violated any of the provisions under this law, as stated in section 23KF (in this chapter – the violator), and intends to impose a monetary sanction on him under that section, he shall provide the violator with written notice of the intention to impose a monetary sanction on him (in this law – notice of intended charge).

(b) In the notice of intended charge, the head of the authority shall indicate, among others, the following:

(1) details of the act constituting the violation, the circumstances of its commission and the date of its commission;

(2) the amount of the monetary sanction and the period for its payment;

(3) the right of the violator to present his arguments before the head of the authority in accordance with the provisions of section 23KI, and that the notice of intended charge shall

be deemed to be a demand for payment if the violator fails to exercise the said right, as detailed in section 23KI(d);

(4) The authority to add to the amount of the monetary sanction due to a continuous or repeated violation under the provisions of section 23L, and the rate of addition.

23KH. Right to Argue

A violator to whom notice of intended charge has been provided in accordance with the provisions of section 23KG may present his arguments, before the head of the authority, in writing or orally, in accordance with 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 aforesaid period, for special reasons to be recorded.

23KI. Decision of the Head of the Authority and Demand for Payment

(a) the head of the authority shall decide, after considering the arguments made under section 23LA, whether to impose a monetary sanction on the violator, and he may reduce the amount of the monetary sanction according to the provisions of section 23LA.

(b) If the head of the authority decides under subsection (a)–

(1) to impose a monetary sanction on the violator – he shall be provided with a demand, in writing, to pay the monetary sanction (in this chapter – a demand for payment), in which he specifies, among others, the amount of the updated monetary sanction and the period for its payment, as well as the right of the violator to file an appeal within 45 days under section 23ME;

(2) Not to impose a monetary sanction on the violator – he shall be notified of this, in writing.

(c) In the demand for payment or in a notice, pursuant to subsection (b), the head of the authority shall specify the reasons for his decision.

(d) If the violator does not present his claims under the provisions of section 23KH within the period mentioned in that section, the notice of intended charge, at the end of that period, shall be deemed to be a demand for payment delivered to the violator on the aforesaid date.

23L. Continuous Violation and Repeated Violation

(a) (1) In a continuous violation, to the monetary sanction specified for that violation the one hundredth part thereof will be added for each day on which the violation continues; in this regard, “continuous violation” means a violation of any of the provisions under this law, as stated in section 23KF, after the violator has been given a demand for payment due to a violation of that provision;

(2) If an appeal is filed against the decision demanding payment, the number of days for the purposes of paragraph (1) shall not be counted for the period until the court decides on the matter, unless the court determines otherwise.

(b) in a repeated violation, an amount equal to the monetary sanction specified for such violation shall be added to the monetary sanction; in this regard, “repeated violation” means a violation of any of the provisions under this law, as stated in section 23KF, committed after the date of payment

of the monetary sanction, within two years of a previous violation of the same provision for which the violator was imposed a monetary sanction or for which he was convicted.

23LA. Reduced Amounts

The head of the authority may not impose a monetary sanction in an amount lower than the amounts specified under this subchapter, except in specified cases and circumstances, and in accordance with the considerations specified in the fifth schedule and at the rates specified therein.

23LB. Updated Amount of the Monetary Sanction

(a) The monetary sanction shall be according to its updated amount on the date of delivery of the payment demand, and in respect of a violator who has not presented his arguments before the head of the authority as stated in section 23KI(d) – on the date of delivery of the notice of intended charge; if an appeal is filed to court and payment of the monetary sanction is stayed by the head of the authority or by the court – the monetary sanction shall be according to its updated amount on the date of the decision on the appeal, as the case may be.

(b) the amounts determined in section 23KF and the amounts set forth in schedule 3, schedule 4, and schedule 5 shall be updated on January 1of each year (in this subsection – the revision date), in accordance with the rate of change in the index known on the revision date compared with the index known on January 1of the previous year; the aforesaid amount shall be rounded up to the nearest amount, which is a multiple of 10 new shekels; the first update under 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 monetary sanction amounts pursuant to subsection (b).

23LC. The Payment Date of the Monetary Sanction

The violator must pay the monetary sanction within 45 days from the date of delivery of the payment demand as stated in section 23KI.

23LD. New Shekel Interest Rate and Late Payment Fees

If the monetary sanction is not paid on time, new shekel interest rate and late payment fees shall be added to it for the period of arrears, until it is paid, and the provisions of the Interest Ruling and Indexation Law, 5721-1961, shall apply with the required changes.

23LE. Collection

A monetary sanction shall be collected to the State Treasury, and its collection shall be subject to the Central Law for the Collection of Fines, Fees and Expenses, 5755-1995.

**Subchapter C: Administrative Alert**

23LF. Administrative Alert

(a) If the head of the authority has reasonable grounds to believe that a person has violated any of the provisions under this Law, as stated in section 23KF, and circumstances determined by the minister of justice exist, the head of the authority may, instead of imposing a monetary sanction on

him under the provisions of subchapter B, give him an administrative alert in accordance with the provisions of this subchapter.

(b) In an administrative alert, the head of the authority will indicate the act constituting the violation, the circumstances of its execution, and the date of its execution, inform the violator that the he must stop the violation and that if he continues or repeats the violation, he will be liable to a monetary sanction for a continuous or repeated violation, as applicable, and the method of calculating the amount of the sanction, as stated in section 23LH, and shall also indicate the right of the violator to request the cancellation of the alert according to the provisions of section 23LG.

23LG. Request to Cancel an Administrative Alert

(a) If an administrative alert is given to the violator as stated in section 23LF, the violator may apply to the head of the authority, in writing, within 45 days, with a request to cancel the administrative alert for any of the following reasons:

(1) the violator did not commit the violation;

(2) The act committed by the violator, specified in the administrative alert, does not constitute a violation.

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

(c) If the head of the authority receives a request to cancel an administrative alert, under the provisions of subsection (a), he may cancel the administrative alert or reject the request and leave the administrative alert as it is; The head of the authority's decision will be given in writing and will be given to the violator together with reasonings.

23LH. Continuous Violation and Repeated Violation After an Alert

(a) If an administrative alert is given to the violator under the provisions of this subchapter and the violator continues to violate the provision for which the alert was given to the him, such violation shall be deemed to be a continuous violation, and the provisions of section 23L(a) shall apply, and the head of the authority shall provide the violator with a notice of intent to charge for the continuous violation in accordance with the provisions of section 23KG, with the required changes.

(b) If an administrative alert is given to the violator under the provisions of this subchapter and the violator repeatedly violates the provision for which the alert was given to him, within two years from the date of delivery of the alert, such additional violation shall be deemed to be a repeated violation for the purposes of section 23L(b), and the head of the authority shall provide the violator with notice of intent to charge for the repeated violation, in accordance with the provisions of section 23KG, with the required changes.

**Subchapter D: Obligation to Refrain from Violation**

23LI. Notice of The Possibility of Submitting a Commitment and a Surety Bond

If the head of the authority has reasonable grounds to believe that a person has violated any of the provisions under this law, as mentioned in section 23KF, and circumstances determined by the minister of justice existed, the head of the authority may give the violator written notice of his possibility of submitting to the head of the authority a letter of commitment and depositing a surety bond under the provisions of this

subchapter, instead of the monetary sanction that may be imposed on him under the provisions of subchapter B.

23M. Terms of Commitment and Amount of Surety Bond

(a) In the letter of commitment, the violator shall undertake to stop the violation of the provision as stated in section 23LI and to refrain from further violation of that provision, within a period determined by the head of the authority and beginning on the date of submission of the letter of commitment, provided that the said period does not exceed two years (in this subchapter – the commitment period).

(b) The head of the authority may determine in the letter of commitment additional conditions that the violator must undertake 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 a surety bond to the authority in the amount of the monetary sanction that the head of the authority was entitled to impose on the violator due to that violation, considering 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 a surety bond under subsection (c) or reduce the amount of the surety bond that the violator deposits under that subsection.

23MA. Results of Submitting a Letter of Commitment and Surety Bond or Non-Submission

(a) If the violator submits a letter of commitment to the head of the authority and deposits a surety bond under this subchapter, within 45 days from the date of delivery of the notice as provided under section 23LI, no monetary sanction shall be imposed for that violation; if the violator does not submit a letter of commitment to the head of the authority or does not deposit surety bond within the said period, the head of the authority shall provide him with a notice of intent to charge for that violation, under section 23KG.

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

23MB. Violation of Commitment

(a) If the violator submits a letter of commitment and deposits a surety bond in accordance with this subchapter and violates any of the terms of the undertaking, as specified in the following paragraphs, the provisions specified in those paragraphs shall apply, as applicable:

(1) If the violator continues, during the commitment period, to violate the provision for which he gave the letter of commitment, or repeatedly violates the said provision during that period, such violation shall be deemed to be a continuous violation under section 23L(a) or as a repeated violation under section 23L(b) and the following provisions shall apply:

(a) The head of the authority shall provide the violator a notice of intent to charge for the continuous or repeated violation, according to the matter, in accordance with the provisions of section 23KG, with the required changes;

(b) If the head of the authority provides the violator with a demand for payment due to the continuous or repeated violation, according to the matter, in accordance with

the provisions of section 23KI(b)(1) or the violator has not made his claims before the head of the authority regarding that violation as determined in section 23KI(d), the head of the authority shall forfeit the surety bond in addition to the imposition of the monetary sanction due to the continuous violation or repeated violation; if the head of the authority decides, under section 23M(d), to exempt the violator from depositing the surety bond or to reduce the amount of the surety bond, the head of the authority shall provide the violator with a payment demand under section 23KI, which also includes the amount of the surety bond for which the exemption was granted or the part reduced from the amount of the surety bond, according to the matter, plus new shekel interest rate, from the date of the decision of the head of the authority on such exemption or reduction until the date of delivery of the payment demand;

(2) If the violator violates any of the additional conditions determined in the letter of commitment under section 23M(b), the head of the authority shall forfeit the surety bond, and if he decides, under section 23M(d), to exempt the violator from depositing the surety bond or to reduce the amount of the surety bond, the head of the authority shall provide the violator with a demand for payment under section 23KI regarding the amount of the surety bond for which the exemption was granted or with respect to the part that was reduced from the amount of the surety bond, according to the matter, plus new shekel interest rate from the date of the decision of the head of the authority on such exemption or reduction until the date of delivery of the payment demand; the head of the authority shall not forfeit the security bond or send a demand for payment under this paragraph unless the head of the authority has given the violator an opportunity to argue his claims, in writing, regarding the violation of such conditions.

(b) Regarding this chapter, the forfeiture of the surety bond according to the provisions of this section shall be deemed as the imposition of a monetary sanction on the violator due to the violation for which the surety bond was given.

(c) If a condition of the terms of the commitment as stated in this section is violated, and the violator again violates the provision for which he gave the letter of commitment, the head of the authority will not allow him to submit another letter of commitment under the provisions of this subchapter, due to that violation.

23MC. Return of Surety Bond

If the violator complies with the terms of the letter of commitment submitted under this subchapter, he will be refunded, at the end of the commitment period, the surety bond plus new shekel interest rate from the date of its deposit until the day of its return.

**Subchapter E: Miscellaneous Provisions Regarding Monetary Sanctions**

23MD. Monetary Sanction for Violation of Several Provisions Under This Law and Under Other Law

For one act that constitutes a violation of several provisions under this law, as well as for an act that constitutes a violation of any of the provisions under section 23KF and of a violation under another law, no more than one monetary sanction shall be imposed.

23ME. Appeal, Delay of Execution, and Refund

(a) The imposition of an administrative enforcement measure in accordance with sections B to E can be appealed to the Magistrate's Court where the President of the Magistrate's Court serves, within 45 days from the date the notice of the action was given.

(b) The submission of an appeal against the decision of the head of the authority in accordance with sections B to E shall not delay the execution of the decision unless the head of the authority agrees to it or the court orders it.

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

(d) If the court decides, after the monetary sanction has been paid or the surety bond has been deposited, to accept an appeal as provided in subsection (a), and has ordered the return of the amount of the monetary sanction paid or the reduction of the monetary sanction or the return of the surety bond, the amount paid or any part thereof that has been reduced or returned will be refunded, according to the matter, plus new shekel interest rate from the date of its payment or deposit until the day of its return.

23MF. Publication

(a) If the head of the authority imposes a monetary sanction in accordance with this chapter, the head of the authority shall publish the following details on the website of the privacy protection authority, in a manner that will ensure transparency regarding the exercise of his discretion in making the decision to impose a monetary sanction:

(1) the imposition of the monetary sanction;

(2) the nature of the violation for which the monetary sanction was imposed, the date of the violation and the circumstances of the violation;

(3) the amount of the monetary sanction imposed;

(4) if the monetary sanction was reduced—the circumstances for which the amount of the monetary sanction and the rates of reduction were reduced;

(5) details about the violator, relevant to the matter;

(6) The name of the violator – if the violator is a corporation, unless it is a corporation managed by an individual and the name of the corporation is the name of its sole owner.

(b) Publication under this section shall not take place until the violator has been given an opportunity to argue his claims; the opportunity to argue claims under this subsection may be given to the violator within the framework of the right to plea under section 23KH, provided that the head of the authority has notified the violator of his intention to publish his name, with a notice of intent to charge under section 23KG.

(c) 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, in the same manner as he published under subsection (a), publish the submission of the appeal and its results.

(d) Notwithstanding the provisions of subsection (a)(6), the head of the authority—

(1) shall not publish the name of the violator who is a corporation, if the head of authority is convinced that the violation is frivolous under the circumstances unless the publication is necessary to warn the public of individuals whose details are in the database;

(2) Publish the name of an individual violator or of a corporation whose name is the name of its sole owner, if it considers it necessary to warn the public.

(e) Notwithstanding the provisions of this section, the head of the authority shall not publish details that constitute data that a public authority is prohibited from disclosing under section 9(a) of the freedom of information law, and he may also refrain from publishing details under this section, which are information that a public authority is not obligated to provide under section 9(b) of the said law.

(f) 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.

(g) The Minister of Justice, with the approval of the constitution committee, may determine additional ways of publishing the details stated in this section.

23MG. Maintaining Criminal Liability

(a) The payment of a monetary sanction, the provision of an administrative alert or the submission of a letter of commitment and the deposit of a surety bond under this chapter shall not detract from the criminal liability of a person for violating any of the provisions under this law which constitutes a criminal offense.

(b) Notwithstanding the provisions of subsection (a), if the violator has been given a notice of intent to charge, an administrative alert or a notice of the possibility of filing a letter of commitment and depositing surety, due to a violation that also constitutes an offense, he shall not be indicted for that violation, unless new facts have been discovered that justify it, as mentioned in section 23IG; new facts as mentioned have been discovered and an indictment has been filed against the violator after the violator has paid a monetary sanction or deposited a surety bond, the violator will be refunded the amount paid or the surety bond deposited, according to the matter, plus new shekel interest rate and late payment fees from the date of payment of the amount or from the date of deposit of the surety, until the day of its return.

(c) If an indictment is filed against a person for an offense that constitutes a violation, the head of the authority shall not take action against the person under subchapters B to E for the violation.

23MH. Delegation of Powers

The head of the authority may delegate his power under subchapters B to E to a senior employee directly subordinate to him and responsible for the domain of monetary sanctions; notice of such delegation shall be published in the Official Gazette.

**Subchapter F: Judicial Cease and Desist Order**

23MI. A Judicial Order to Stop Processing or an Order to Delete Personal Data

(a) If the head of the authority has reasonable grounds to believe that a violation of provisions under section 2(9), 8(b), (c) or (d), 17 or 23B is being committed in the database, he may request an

administrative court (in this section – the court) to issue an order to the database controller of the database or to the database holder, to stop processing activities that cause a violation or there is a concern that they will cause a violation (in this section – a cease and desist order), and for this purpose the court may order the deletion of the personal data in the database in its entirety (in this section – a deletion order).

(b) The court may issue an order under subsection (a), as requested or modified, if it is satisfied that all of the following have been fulfilled:

(1) there are reasonable grounds to believe that a violation as provided in that subsection is or is about to be committed in the database;

(2) there is no other lesser means of preventing the commission of the violation;

(3) the damage that may be caused as a result of the violation exceeds the damage that may be caused by the issuance of the order relating to it, including the violation of freedom of expression that may be caused by the issuance of the order;

(4) The severity of the violation justifies the issuance of the order.

(c) (1) An order under this section shall be issued after the database controller of the database has been given an opportunity to claim his arguments before the court, and if the order is directed against the holder – also to the holder, to the extent possible, and in the appropriate manner under the circumstances;

(2) An order of termination without the presence of a party as provided in paragraph (1) shall be issued for a period not exceeding 48 hours; during such period, no deletion order shall be issued;

(3) The court may extend the validity of the order after the database controller of the database or the database holder, according to the matter, has been given an opportunity to voice his arguments.

(d) The court may reconsider an order under this section if it considers it justified by changed circumstances or new facts discovered after the order was issued.

(e) A proceeding under this section shall be governed by the provisions of the Administrative Courts Law, 5760-2000, with the necessary modifications; the Minister of Justice, with the approval of the constitution committee, may make provisions regarding procedures in a proceeding under this section; until such provisions are determined, the provisions of the Citizenship Regulations (procedures for application to revoke citizenship), 5777-2017, shall apply with the necessary changes.

**CHAPTER D'4: Enforcement and Penal Powers**

**Subchapter A: Enforcement Powers**

23N. Appointment of Investigators

(a) The head of the authority may authorize an investigator from among the civil servants, who will have the powers or part of them under this law (hereinafter: an investigator), if all of the following have been fulfilled:

(1) The Israeli Police announced, within three months of the head of the authority's request to it, that it does not object to his certification for reasons of public safety, including because of his criminal record;

(2) He received appropriate training in the domain of the powers that will be given to him under this law, and has met additional qualifications, to the extent prescribed, as instructed by the minister of justice with the consent of the minister of national security, and with regard to the exercise of powers to access or copy computer material as stated in section 23NA(a)(3) – he is an official skilled in carrying out such activities;

(3) He has received appropriate training in the domain of privacy protection, as directed by the minister of justice.

(b) The certification of an investigator under this section shall be in a certificate signed by the head of the authority, attesting to his role as an investigator and his powers under this law (hereinafter: an investigator's certificate).

(c) Notice of certification under subsection (b) shall be published in the official gazette and on the website of the privacy protection authority.

23NA. Enforcement Powers

(a) If the investigator has reasonable grounds to suspect that an offense has been committed under section 5, in the circumstances detailed in section 2(9), and the suspicion is that the offense was committed in connection with knowledge of a person's private affairs in a database, or the investigator had reasonable grounds to suspect that an offense has been committed under chapter B or under this chapter, he may-

(1) investigate any person connected with such an offense or who may have information relating to such an offense; an investigation under this paragraph shall be governed by the provisions of sections 2 and 3 of the Criminal Procedure Ordinance (Testimony) and the provisions of the Criminal Procedure Law (Interrogation of Suspects), 5762-2002, with the necessary modifications;

(2) seize any object which has reasonable grounds to believe that it is an object connected with such an offense;

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

(b) For searching, seizing an object and accessing or copying computer material under this section, 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, with the following changes: the powers given to the police officer shall be given to the investigator and the powers given to the police sub-Inspector shall be given to the head of the authority or the investigator authorized to do so; notice of accreditation under this subsection shall be published official gazette and on the authority's website.

(c) (1) If an investigator has reasonable grounds to suspect that a person has committed an offense as stated in subsection (a), the investigator may detain the person in order to ascertain the person identity and address or to interrogate him at his whereabouts; if the identification is insufficient or the person cannot be interrogated at his location, the investigator may require that person to accompany him to the offices of the authority or to

summon the person to the offices of the authority for another date to be determined; whoever has been summoned to the offices of the authority shall appear at the time summoned to him;

(2) For a delay under paragraph (1), the provisions of sections 66, 67 and 72 to 74 of the Arrests Law shall apply, with the necessary modifications, and with the following changes: The powers given to the police officer shall be given to the investigator and the powers given to the police sub-Inspector shall be given to the head of the authority or to the investigator authorized to do so, and the offices of the authority declared by the head of the authority by a notice in the official gazette shall be deemed to be a police station for the purposes of the provisions of the arrests law.

23NB. Investigator Identification

(a) An investigator shall not use the powers granted to him under this subchapter except in the performance of his duties and in fulfillment of the following two:

(1) Provisions regarding the identification of an inspector under section 23JA are complied, with the necessary changes;

(2) He wears an investigator's uniform, in the color and form instructed by the head of the authority for this purpose, provided that such uniform does not pretend to be a police uniform.

(b) The provisions of section 23JB(b) and (c) shall apply, with the necessary changes, with respect to the obligations stated in subsection (a).

**Subchapter B: Offenses**

23NC. Interfering With The Head Of The Authority, Investigator, Or Supervisor In The Performance Of Duties

Obstructing the head of the authority, investigator or inspector in the performance of duties under this law shall be punishable by imprisonment for six months.

23ND. Misleading The Head Of The Authority, an Inspector, Or an External Expert

Whoever does any of the following with the intention of misleading the head of the authority, an inspector, or an external expert, is sentenced to two years imprisonment:

(1) 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);

(2) provides incorrect information in response to a requirement of an inspector under section 23J(a)(1)-(3) or of an external expert under section 23JH(f).

23NE. Processing Data From a Database Without Authorization

The one who is processing personal data from a database without authorization from the database controller, contrary to the provisions of section 8(c), is sentenced to imprisonment of three years.

23NF. Providing Incorrect Information When Requesting Data

The one who is contacting a person to receive personal data for the purpose of processing the data in a database and providing him with incorrect details, contrary to the provisions of section 11, with the intention of misleading him regarding the provision of the personal data, is sentenced to imprisonment of three years.

23NG. Unlawful Data Transfer From a Public Body

A public body as defined in section 23 is a corporation, an employee of such a public body or a person acting on behalf of such a public body, who provides personal data whose transfer is prohibited under the provisions of section 23B, In order for an unauthorized party to process the data, is punishable by imprisonment of three years.

**CHAPTER D'5: Provisions Regarding Elections**

23NH. Definitions

In this chapter –

"general elections for authorities" – general elections within the meaning of section 4 of the Local Authorities Law (elections);

"local authority elections" – elections as defined in the Local Authorities Law (Elections) or the Regional Councils Law (Date of General Elections), 5754-1994, excluding elections to the local committee of a locality in a regional council;

"Central Elections Committee" – within the meaning of the Elections for the Knesset Law [Consolidated Version], 5729-1969;

"The Elections Law (Ways of Propaganda)" – Elections Law (Ways of Propaganda), 5719-1959;

"The Regional Councils Law" – The Regional Councils Law (Election of the Head of the Council), 5748-1988;

"The Local Authorities (Elections) Law" – The Local Authorities (Elections) Law, 1965;

"Chairman of the Regional Election Committee" means the chairman of a regional election committee determined under section 17D of the Elections Law (Ways of Propaganda), regarding elections for a local authority within the jurisdiction of the district court in which he serves;

"Candidate in municipal elections" – any of the following:

(1) From the beginning of the period of the general elections until the day the lists are submitted-

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

(b) a faction of an outgoing council, within the meaning of section 25 of the Local Authorities (Elections) Law;

(c) a person who is entitled, under section 16(b)(1) of the Local Authorities (Elections) Law, to receive

in a passbook, and the information is provided to him under section 16(c) of the said law;

(d) A person who is entitled, in accordance with section 5B(a)(1) of the Regional Councils Law, to receive information in the passbook, and the information is provided to him in accordance with the said section;

(2) As of the date of submission of lists of candidates – a list of candidates in elections to the council of a local authority and a candidate for head of a local authority, as well as a person who submitted the list of candidates or the candidate's proposal, excluding a group of voters;

"Party" – as defined in the Parties Law, 5752-1992, and regarding the part of the pre-elections period for the Knesset beginning on the day following the deadline for submitting a list of candidates for the Knesset to the Central Elections Committee – such party that has submitted a list of candidates participating in the Knesset elections;

"Pre-election periods" – the period of elections to the Knesset or the period of general elections to the authorities;

"General pre-election period for municipalities" means a period beginning on the 101st day before the day of the general elections for the local authorities, and ending on the 14th day after said election day;

"Pre-elections period for the Knesset" – a period that begins on the determining day, as defined in the Financing Parties Law, 5733-1973, and ends on the day of publication of the election results pursuant to section 11 of The Knesset Basic Law;

"Authority's pre-election periods – a period that begins on the day of submission of lists of candidates or candidate proposals and ends on the 14th day after Election Day.

23NI. Exercising Powers Under chapters D'1 and D'3 During Pre-Election Periods

(a) The head of the authority, supervisor or investigator shall not, during pre-election periods, exercise the power granted to him under the sections listed below due to a violation of any of the provisions under this Law, relating to a database in which a party or candidate in elections for a local authority is the controller, which they or a holder carried out, unless he has received approval under subsection (b):

(1) entering a place under section 23J(a)(4);

(2) submitting an application for a search and seizure warrant or a computer material access warrant as part of an administrative investigation, pursuant to section 23JD;

(3) filing an application for a cease-and-desist order under section 23MI;

(4) power to seize any object, pursuant to section 23NA(a)(2);

(5) filing an application for a search and seizure warrant or a computer material access warrant, pursuant to section 23NA(a)(3);

(6) notice of intent to charge under section 23KG;

(7) the provision of an administrative alert, under section 23LF;

(8) Providing a notice of the possibility of submitting a letter of commitment and depositing a surety bond, under section 23LI.

(b) A power referred to in subsection (a) may be exercised—

(1) During the pre-elections period for the Knesset, regarding a database that a party as defined in the Local Authorities Law is the controller of – with the approval of the chairman of the Central Elections Committee;

(2) During the general pre-election period for the authorities, with regard to a database in which a party as defined in the Local Authorities Law (Elections) or a faction of the Knesset has control of – with the approval of the chairman of the Central Elections Committee, and with regard to a database in which another candidate in local elections is the controller – with the approval of the chairman of the regional elections committee.

(c) Before granting approval under this section, the chairman of the Central Elections Committee or the chairman of the regional election committee, according to the matter, shall give an opportunity to the party or candidate in the elections of the local authority concerned to argue their claims; however, with respect to a power under subsections (a)(1) to (5), the chairman of such an election committee may grant approval for the exercise of the authority without asking for the position of the party or candidate in the local authority elections, for reasons of urgency or if this would thwart the purpose of exercising the requested authority; the circumstances of the case and the reasons for urgency will be detailed in the decision of the Chairman.

(d) The chairman of the central elections committee or the chairman of a regional election committee shall not give approval for the exercise of authority under this section, if he finds that doing so will materially impair the ability of the party or candidate in the local authority elections, according to the matter, to run in the elections or to manage contact with the electorate, and that the intensity of such anticipated violation exceeds the risk of invasion of privacy and the risk of harm to the public interest underlying the exercise of the authority; such approval may be conditional.

(e) The chairman of the central elections committee and the chairman of the regional elections committee discussing a particular application may, on their own initiative, or upon a request by a party involved in a legal proceeding that was submitted before or during the commencement of the hearing, order that the hearing be held before the chairman of the central elections committee, if they consider it justified in the circumstances.

(f) If the head of the authority, an inspector or an investigator decides to exercise authority under this section during the general pre-election period for municipalities held on a day other than the day of the general elections for the authorities, regarding a database in which the candidate in the elections for a municipalities is the controller of, the candidate in the elections for a municipality may request from the chairman of a regional election committee, and if he is a party as defined in the local authorities law (elections) or a faction of the Knesset – from the chairman of the central elections committee, to determine that the said authority will not be exercised during the election period for that local authority, if it is found that the provisions of subsection (d) have been fulfilled, or to condition the exercise of powers on conditions; such request and decision shall be governed by the provisions of subsections (c) and (e), with the required changes.

(g) Proceedings under this section shall be governed by the provisions of sections 17D and 17E of the Elections Law (Ways of Propaganda), with the necessary modifications.

(h) The provisions of this section shall apply, with the necessary changes, also regarding elections to another local authority or to another regional council budgeted from the state budget, except for a local committee.

**Chapter E: Miscellaneous**

24. State Applicability

This law applies to the state.

25. Death of the Injured Party

(a) Where a person whose privacy has been invaded dies within six months of the invasion without having filed a claim or complaint in respect of that invasion, his spouse, child, or parent, or if he left no spouse, children, or parents – his sibling, may file a lawsuit or complaint for that invasion within six months of his death, file a claim or complaint in respect of that invasion.

(b) Where a person who has filed a claim or complaint for a privacy invasion dies before the conclusion of the proceedings, his spouse, child or parent, or if he leaves no spouse, children or parents – his sibling, may inform the court, within six months of his death, of their will to proceed the claim or complaint, and upon the said notification, he or she shall be substituted as the plaintiff or complainant.

26. (Revoked)

27. Applicability of the Prohibition of Defamation Law Provisions

The provisions of sections 21, 23 and 24 of the Prohibition of Defamation Law, 5725-1965, shall apply, as applicable, to legal proceedings for privacy invasion.

28. Evidence of a Person's Bad Reputation, Character, or Past

In criminal or civil proceedings for privacy invasion, no evidence shall be brought, nor shall any witness be examined, regarding the bad reputation of the injured party or as to his character, past, actions or opinions.

29. Additional Orders

(a) In addition to any other penalty or remedy, the court may, in criminal or civil proceedings for violation of any provision of this law, order as specified below, as the case may be:

(1) Prohibition of the distribution of copies of the harmful material or confiscate it; an order of confiscation under this paragraph shall be effective against any person in whose possession such material is found for the purpose of sale, distribution, or storage, even if that person was not a party to the proceedings; where the court orders confiscation, it shall direct how the confiscated copies shall be disposed of;

(2) Publication of the judgment, in whole or in part; the publication shall be at the expense of the accused or defendant, in the place, extent, and manner determined by the court;

(3) Delivering the harmful material to the injured party.

(4) Destruction of unlawfully obtained data, or prohibition of the use of said data or excessive data as defined in section 23E, or order any other instruction regarding the data.

(b) The provisions of this section shall not prohibit the retention of a copy of a publication in public libraries, archives, or similar institutions, except where a court, under subsection (a)(1), issues a confiscation order which also imposes restrictions on such retention. Furthermore, the provisions of this section shall not prohibit the retention of a copy of a publication by an individual.

29A. Statutory damages

(a) If a person has been convicted of a Criminal offense under section 5, the court may order him to pay the injured party monetary compensation not exceeding 50,000 new shekels, without proof of damage; an order for compensation under this subsection shall be regarded as a ruling issued by a court in a civil lawsuit of the entitled person against the debtor.

(b) (1) In a civil proceeding under section 4, the court may award monetary compensation to the injured, not exceeding 50,000 new shekels, without proof of damages;

(2) In a civil proceeding under paragraph (1), where it is proven that the privacy invasion was committed with an intent to cause harm, the court may award monetary compensation to the plaintiff, not exceeding twice the amount specified in the said paragraph, without proof of damage.

(c) No person shall be awarded monetary compensation without proof of damage under this section for the same privacy invasion more than once.

(d) The amounts specified in this section shall be updated on the 16th of each month, in accordance with the rate of change in the New Index compared to the Base Index. For this purpose:

"Index" – the Consumer Price Index published by the Central Bureau of Statistics;

"New Index" – the index of the month preceding the month of updating;

"Base Index" – the index of the month of May 2007.

30. Liability Resulting from Newspaper Publication

(a) If a privacy invasion is published in a newspaper, the person who brought the matter to the newspaper and thereby caused its publication, the editor of the newspaper, and the person

who made the final decision to publish the privacy invasion, shall bear criminal and civil liability for the Invasion, and the publisher shall also be held civilly liable.

(b) In a criminal charge according to this section, it shall be a valid defense for the editor of the newspaper if he took reasonable measures to prevent publication of said invasion or were unaware of its publication.

(c) In this section, "editor" of a newspaper includes the actual editor.

31. Liability of Printer and Distributor

Where a privacy invasion is published in print, except in a newspaper published at a frequency of forty days or less, criminal and civil liability for the invasion shall also be borne by the holder of the printing house in which the invasion was printed, and by any person who sells or otherwise distributes the publication; provided that they shall not bear liability unless they had or should have had knowledge that the publication contained a privacy invasion.

31A. (Revoked)

31B. Tortious Action

An act or omission in violation of the provisions of chapters B or D, or in violation of Regulations enacted under this Law, shall constitute a tortious act under the Civil Wrongs Ordinance [New Version]

32. Inadmissible Evidence

Material acquired through a privacy invasion shall be inadmissible as evidence in court, absent the consent of the injured party, unless the court, for reasons to be recorded, permits its use, or if the violator, being a party to the proceeding, has a valid defense or is exempt under this Law.

33. Amendment of the Civil Wrongs Ordinance

In the Civil Wrongs Ordinance [New Version], section 34A – repealed.

34. Amendment of the Criminal Procedure Law

In the schedule to the Criminal Procedure Law, 5725-1965, the following shall be inserted after paragraph (12):

"(13) Offenses under the Privacy Protection Law, 5741-1981."

35. Preservation of Laws

The provisions of this Law shall not derogate from the provisions of any other law.

36. Implementation and Regulations

The minister of justice shall be responsible for the implementation of this law and may establish regulations, with the approval of the Constitution Committee, in all matters related to its implementation, including:

(1) Conditions for data retention and its storage in databases;

(2) Conditions for the transfer of data to or from databases located outside the borders of the state;

(3) Rules of conduct and ethics for controllers or holders of databases and their employees;

(4) Provisions for data deletion upon the termination of a database's operation.

36A. Fees

(a) The minister of justice may, with the approval of the Constitution Committee, establish fees for database review under this Law.

(b) (Revoked)

(c) (Revoked)

36B. Amendment of schedules

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.

37. Commencement

chapter B shall come into force six months from the date of publication of this Law.

**Schedule 1**

(The definition of "the Authority" - "the Privacy Protection Authority" in section 3)

**Wording of Government Decision No. 1890**

Subject of the Decision:

Independence of the Privacy Protection Authority and Amendment of a Government Decision

It is decided:

1. (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 purpose of fulfilling its functions through the employees of the Authority and in accordance with the provisions of any law, and the budget for the Authority's activities shall be managed separately within the budget of the Ministry of Justice. Out of respect for the independence of the Authority, the Authority shall act independently when exercising the powers vested in the Head of the Authority.

2. The functions of the Authority are, among others, the following:

   (a) To supervise compliance with the provisions of the Privacy Protection Law, 5741-1981, and the Regulations thereunder with respect to databases;

(b) To investigate suspicions of the commission of offenses under the Privacy Protection Law, 5741-1981, with respect to databases in accordance with its powers under the law;

(c) 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 advocacy;

(d) To handle public inquiries that have merit regarding harm to data subjects under the Privacy Protection Law, 5741-1981;

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

(f) To promote and maintain relations with counterpart bodies in the world and within the framework of international forums in which counterpart bodies participate;

(g) To exercise the powers of the Registrar of Authorized Bodies under the Electronic Signature Law, 5761-2001.

3. (a) Further to Government Decisions No. 4660 of 19.1.2006 and No. 3543 of 11.2.2018, it is determined that the qualifications for appointment as Head of the Authority shall be as follows:

(1) A person who meets the qualifications for appointment as a judge of the District Court;

(2) A person who has been convicted of a criminal offense or a disciplinary offense which, by its nature, severity, or circumstances, renders him 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 rendered in his case, shall not be appointed as Head of the Authority.

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

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

(a) The Government shall appoint the Head of the Authority by notice in the Official Gazette as Registrar for the purposes of section 7 of the Privacy Protection Law, 5741-1981;

(b) The minister of justice shall appoint the Head of the Authority as Registrar for the purposes of section 9 of the Electronic Signature Law, 5761-2001.

**Schedule 2**

(paragraph (12) of the definition "data of special sensitivity", in section 3)

(1) Data about membership in a workers' organization as stated in Regulation 7 of the Privacy Protection Regulations (Instructions regarding data transferred to Israel from the European Economic Area), 2023.

**Schedule 3**

(section 23Kf(h))

**Monetary Sanction for Violating the Data Security Regulations**

In this schedule –

"External entity" – as defined in Regulation 15(a) of the Regulations;

"Individual" – a person and his relative, a person and his legal representative; for this purpose "relative" – spouse, sibling, parent, grandparent, offspring, and the spouse of any of these, as well as the offspring of a sibling, and the sibling of a parent;

"Database managed by an individual" – a database that the database controller thereof is an individual or a corporation owned by an individual or a corporation owned by two individuals, and that no more than two additional authorized persons are authorized to make use of it, but excluding the following databases:

(1) A database whose primary purpose is to collect personal data for the transfer thereof to another as a business practice or for consideration, including direct mailing services;

(2) A database containing personal data about 10,000 or more individuals;

(3) A database containing personal data for which the database owner is subject to a professional duty of confidentiality under law or professional ethical principles;

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

(1) Its primary purpose is not to collect personal data for transfer to another as a business practice or for consideration, including direct mailing services;

(2) The database controller is not a public body as defined under section 23;

(3) If the database contains data of special sensitivity, one of the following also applies:

(a) The number of authorized persons at the database controller does not exceed ten;

(b) The database includes data of special sensitivity only about the database controller's employees or suppliers, is used solely for managing the database controller's business, and is only of one of the following types:

(1) data according to paragraphs (2), (6), and (8) to (10) of the definition "data of special sensitivity";

(2) Personal data about the employees' sexual orientation or his spouse's, deriving from data provided by the employee;

(3) Personal data about his religious beliefs;

(4) Personal data that is a biometric identifier as aforesaid under paragraph (4) to the definition of "data of special sensitivity" that is a facial image only;

"Database subject to the intermediate security level" – a database that is not a database managed by an individual, is not a database subject to the high security level, and that meets one of the following:

(1) Its primary purpose is to collect data for transfer to another as a business practice or for consideration, including direct mailing services;

(2) The database controller is a public body as defined in section 23;

(3) The database includes data of special sensitivity, except for data of special sensitivity excluded in paragraph (3)(b) of the definition of a "database subject to the basic security level";

"Database subject to the high security level" – a database that meets one of the following:

(1) A database as stated in item (1) to the definition of a "database subject to the intermediate security level" or a database containing data of special sensitivity where the number of authorized persons at the database controller exceeds 100 or that contains personal data about 100,000 or more individuals;

(2) A database containing biometric identifiers of 100,000 or more individuals;

"Data Security Regulations" – Protection of Privacy Regulations (Data Security) 5777-2017.

| Violation | Monetary sanction Sum | | | |
|---|---|---|---|---|
| Column A | Column B – a database managed by an individual | Column C – a database subject to basic security level | Column D – a database subject to intermediate security level | Column E – a database subject to high security level |
| (1) Preparation of the database definitions document: A database controller that has not defined in the database definitions document all the matters referred to in Regulation 2(a) of the Data Security Regulations, in violation of the provisions of that Regulation, including the different types of data contained in the database pursuant to sub-Regulation (3), taking into account the list of types of data that constitute data of special sensitivity pursuant to section 3 of the law. | 2,000 | 2,000 | 40,000 | 160,000 |
| (2) Updating the database definitions document: A database controller that has not updated the database definitions document, in violation of the provisions of Regulation 2(b) of the Data Security Regulations. | 2,000 | 2,000 | 40,000 | 160,000 |

| | | | | |
|---|---|---|---|---|
| (3) Excess data review: A database controller that has not examined or documented the examination of whether the data it holds in the database is not excessive for the purposes of the database, in violation of the provisions of Regulations 2(c) or 19(b) of the Data Security Regulations. | 2,000 | 2,000 | 40,000 | 160,000 |
| (4) Preparation of an data security procedure: A database controller or database holder that has not established under a document a data security procedure in accordance with the database definitions document and the Data Security Regulations (hereinafter – security procedure), in violation of the provisions of Regulation 4(a) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) of the aforementioned Regulations, as the case may be. | – | 2,000 | 40,000 | 160,000 |
| (5) Security procedure – preparation, maintenance, and setting instructions: A database controller or database holder that has not done one of the following:<br>(a) Maintained the security procedure so that details from it are provided to authorized persons only to the extent necessary for the performance of their duties, in violation of the provisions of Regulation 4(b) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) of the aforementioned Regulations, as the case may be;<br>(b) Included in the security procedure the details listed in Regulation 4(c) of the Data Security Regulations; and regarding a database to which the medium or high security level applies – included in it a reference to the details listed in Regulation 4(d) of the Data Security Regulations or the provisions referred to in Regulation 9(b)(2) of the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) of the aforementioned Regulations, as the case may be;<br>(c) Set in the security procedure instructions regarding handling of data security incidents or regarding reporting to the database controller, in violation of the provisions of | – | 2,000 | 40,000 | 160,000 |

| | | | | |
|---|---|---|---|---|
| Regulation 11(b) of the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) of the aforementioned Regulations, as the case may be;<br>(d) Detailed in the security procedure the matters listed in Regulation 15(a)(2)(a) to (e) of the Data Security Regulations, in violation of the provisions of Regulation 15(a)(3) of the aforementioned Regulations. | | | | |
| (6) Database structure and systems: A database controller or database holder that has not maintained an updated document of the database's structure or an updated inventory list of the database's systems, in accordance with the provisions of Regulation 5(a) of the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) of the aforementioned Regulations, as the case may be. | – | 1,000 | 20,000 | 80,000 |
| (7) Provision of details on the database's structure and inventory list: A database controller or database holder who has not kept the updated database structure document or the inventory list according to the access permissions set in accordance with the provisions of Regulation 5(b) of the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) of the aforementioned Regulations, as the case may be. | – | 1,000 | 20,000 | 80,000 |
| (8) Protection of systems: A database controller or database holder that has not ensured that the systems specified in Regulation 5(a)(1) of the Data Security Regulations are stored in a secure place that prevents access and entry without authorization, in a manner appropriate to the nature of the database's activity and the sensitivity of the data contained therein, in accordance with the provisions of Regulation 6(a) of the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) of the aforementioned Regulations, as the case may be. | 1,000 | 1,000 | 20,000 | 80,000 |
| (9) Risk assessment: A database controller or database holder that has not ensured that a risk assessment to identify data security risks is conducted at least once every 18 months (hereinafter – risk assessment), or that has not discussed the results of the risk assessment that were provided to it | – | – | – | 320,000 |

| | | | | |
|---|---|---|---|---|
| and that has not examined the need to update the database definitions document or the security procedure as a result thereof, or that has not acted to correct deficiencies identified as part of the risk assessment, in violation of the provisions of Regulation 5(c) of the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | | | | |
| (10) Penetration tests: A database controller or database holder that has not ensured that penetration tests are conducted on the database's systems at least once every 18 months, or that has not discussed the results of the penetration tests or that has not acted to correct deficiencies identified, in violation of the provisions of Regulation 5(d) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | – | – | – | 320,000 |
| (11) Control and documentation of site access: a database controller or database holder that has not taken measures for control and documentation in accordance with the provisions of Regulation 6(b) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | – | – | 20,000 | 80,000 |
| (12) Human resources management: A database controller or database holder that has granted access to data contained in the database or changed the scope of the authorization granted, without taking any reasonable measures as referred to under Regulation 7(a) to the Data Security Regulations, in violation of the provisions of that Regulation or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the Data Security Regulations, as the case may be. | – | 1,000 | 20,000 | 80,000 |
| (13) Human resources training: A database controller or database holder that has granted access to data contained in the database or changed the scope of the authorization granted, without first providing training or providing data to authorized persons as required, in violation of the provisions of Regulation 7(b) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in | – | 1,000 | 20,000 | 80,000 |

| | | | | |
|---|---|---|---|---|
| Regulation 19(a) to the aforementioned Regulations, as the case may be. | | | | |
| (14) Periodic training: A database controller or database holder that has not conducted periodic training activities for its authorized personnel, in violation of the provisions of Regulation 7(c) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | – | – | 20,000 | 80,000 |
| (15) Establishment and management of access permissions: A database controller or database holder that has not established access permissions for authorized persons to the database and the database's systems, in violation of the provisions of Regulation 8(a) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the Data Security Regulations, as the case may be, or has not maintained an updated record of valid permissions, in violation of the provisions of Regulation 8(b) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be (hereinafter - list of valid permissions). | – | 2,000 | 40,000 | 160,000 |
| (16) Implementation of access permission procedure: A database controller or database holder that has not taken acceptable measures under the circumstances and in accordance with the nature and type of the database, in order to ensure that access to the database and database's systems is made only by an authorized person according to the list of valid permissions, in violation of the provisions of Regulation 9(a) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | 2,000 | 2,000 | 40,000 | 160,000 |
| (17) Implementation of access permission procedure with respect to an authorized person who has finished his role: A database controller or database holder that has not ensured the cancellation of permissions granted to an authorized person who has finished his role, in violation of the provisions of Regulation 9(c) to the Data Security Regulations or the provisions of the aforementioned Regulation as | – | 2,000 | 40,000 | 160,000 |

| | | | | |
|---|---|---|---|---|
| applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | | | | |
| (18) Access control and documentation mechanism: A database controller or database holder that has not done one of the following:<br>(a) Ensured that a control mechanism is maintained, in violation of the provisions of Regulation 10(a) and (b) to the Data Security Regulations (hereinafter – control mechanism) or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be;<br>(b) Established a routine inspection procedure of the documentation data of the control mechanism and prepared a report of problems identified and steps taken as a result thereof, in violation of the provisions of Regulation 10(c) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be;<br>(c) Ensured that documentation data of the control mechanism is kept for at least 12 months, in violation of the provisions of Regulation 10(d) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be;<br>(d) Informed the authorized persons in the database of the existence of the control mechanism, in violation of the provisions of Regulation 10(e) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | – | – | 40,000 | 160,000 |
| (19) Data security event documentation: A database controller or database holder that has not ensured the documentation of any case in which an event occurred that raises concern of damage to the integrity of data, unauthorized use thereof, or exceeding authorization (hereinafter – data security events), in violation of the provisions of Regulation | 2,000 | 2,000 | 40,000 | 160,000 |

| | | | | |
|---|---|---|---|---|
| 11(a) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | | | | |
| (20) Periodic discussion on data security incidents: A database controller or database holder that has not held a discussion on data security incidents or has not examined the need to update the security procedure and documented such discussion and examination, in violation of the provisions of Regulation 11(c) and Regulation 19(b) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | – | – | 40,000 | 160,000 |
| (21) Reporting to the authority regarding a serious security incident: A database controller or database holder that has not immediately notified the head of the authority of a serious security incident, or has not reported to the head of the authority on the steps taken as a result of the event, in violation of the provisions of Regulation 11(d)(1) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | – | – | 80,000 | 320,000 |
| (22) Updating the database's systems: A database controller or database holder that has not ensured that regular updates are conducted to the database's systems, including computer material required for their operation, or that systems that are not supported by the manufacturer in terms of their security aspects are not used without any security consideration, in violation of the provisions of Regulation 13(c) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | 2,000 | 2,000 | 40,000 | 160,000 |
| (23) Network connection security: A database controller or database holder that has connected the database's systems to the internet or another public network without installing any protective measures, in violation of the provisions of Regulation 14(a) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | 2,000 | 2,000 | 40,000 | 160,000 |

| | | | | |
|---|---|---|---|---|
| (24) Control and supervision of an external party (outsourcing): A database controller that has entered into an agreement with an external party to provide services, that has not explicitly stated in the agreement with the external party the matters listed in Regulation 15(a)(2) to the Data Security Regulations or has not taken any control and supervision measures over the external party's compliance with the provisions set forth in the aforementioned agreement regarding the matters detailed in subparagraphs (d) and (f) to (h) to the aforementioned Regulation, in violation of Regulation 15(a)(4) to the Data Security Regulations. | – | 4,000 | 80,000 | 320,000 |
| (25) Documentation: A database controller or database holder that has not stored in a secure manner, for at least one year, the data accumulated in the course of implementing the provisions of Regulations 6(b), 8-11, 14, 15(a)(4) and 16 to the Data Security Regulations, that apply to it, in violation of the provisions of Regulation 17(a) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the Data Security Regulations, as the case may be. | – | 1,000 | 20,000 | 80,000 |
| (26) Backup of documentation data: A database controller or database holder that has not done one of the following:<br>(a) Backed up retained data in such a manner that will ensure the possibility, at any time, to restore the data to its original state, in violation of the provisions of Regulation 17(b) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be;<br>(b) Established in a document the matters listed in Regulation 18(a)(1) and (3) to the Data Security Regulations and that has also established procedures to ensure data recovery, as referred to in Regulation 17(b) to the aforementioned Regulations;<br>(c) Ensured that a backup copy of the data and the procedures referred to in Regulation 18(a) of the Data Security Regulations is retained in a manner that will ensure the integrity of the data and the possibility of restoring the data, | – | – | 20,000 | 80,000 |

| | | | | |
|---|---|---|---|---|
| in violation of the provisions of Regulation 18(b) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | | | | |
| (27) Violation of documentation obligations: A database controller or database holder that has not documented the manner in which it performs an activity that is not the creation of a document, which it is obligated or responsible to perform under the Regulations, in violation of the provisions of Regulation 19(b) to the aforementioned Regulations. | – | 1,000 | 20,000 | 80,000 |
| (28) Segregation of the database's systems (compartmentalization): A database controller or database holder that has not separated between the database's systems that can be used to access personal data and other computer systems used by it, in violation of the provisions of Regulation 13(b) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | – | – | 20,000 | 80,000 |
| (29) Periodic audit: A database controller or database holder that has not ensured that an internal or external audit is conducted at least once every 24 months, in violation of the provisions of Regulation 16(a) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be, or has not discussed the audit reports that were provided to it, or that has not examined the need to update the database definitions document or the security procedure as a result thereof, in violation of the provisions of Regulation 16(c) to the Data Security Regulations or the provisions of the aforementioned Regulation as applied in Regulation 19(a) to the aforementioned Regulations, as the case may be. | – | – | 40,000 | 160,000 |

**Schedule 4**

(section 23Kf(i))

**Monetary Sanction for Violating Regulations Regarding the Transfer of Data From the EEA**

In this Appendix, "Regulations for the Transfer of Data from the European Economic Area" – the Protection of Privacy Regulations (Provisions Regarding Data Transferred to Israel from the European Economic Area), 5789-2023.

**Part A**

| Column A<br>The Violation | Column B<br>Monetary sanction Sum |
|---|---|
| (1) A database controller that has not provided written notice to the data subject of its decision regarding a request under the provisions of Regulation 3(a) to the Regulations for the Transfer of Data from the European Economic Area, in violation of the provisions of Regulation 3(d) to the aforementioned Regulations. | 15,000 new shekels |
| (2) A database controller that has not implemented any organizational, technological, or other mechanism, whose purpose is ensuring that the database does not retain data that is no longer necessary for the purpose for which it was collected or retained or for another purpose for which it is permitted to be retained under any law (hereinafter – unnecessary information), in violation of the provisions of Regulation 4(a) to the Regulations for the Transfer of Data from the European Economic Area. | An amount of 2 new shekels for each person about whom personal data is retained in the database, and if the personal data in the database was data 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 aforementioned data was data of special sensitivity – less than 40,000 new shekels, the head of the Authority may impose a monetary sanction on a database controller or a database holder in the amount of 20,000 new shekels or 40,000 new shekels, as the case may be. |
| (3) A database controller that has not implemented any organizational, technological, or other mechanism whose purpose is ensuring that the data in the database is accurate, complete, clear, and up-to-date, in violation of the provisions of Regulation 5(a) to the Regulations for the transfer of information from the European Economic Area. | |
| (4) A database controller that has found that the database holds data that is not accurate, complete, clear, or up-to-date, and that has not taken any measures to correct or delete the information, in violation of the provisions of Regulation 5(b) to the Regulations for the transfer of information from the European Economic Area. | |

**Part B**

| | |
|---|---|
| (1) A database controller that received a written request for the deletion of personal data as referred to in Regulation 3(a) to the Regulations for the Transfer of Data from the European Economic Area, and the exceptions as referred to in Regulation 3(b) of the aforementioned Regulations did not apply, and that did not erase the data or take actions to ensure that it will not be possible, by reasonable means, to identify the data subject, in violation of the provisions of Regulation 3(c) to the aforementioned Regulations, and this after receiving a notice from the head of the authority under section 23ka(c), that its actions constitute a violation, and it did not cease the violation within the period instructed by the head of the authority. | An amount of 4 new shekels for each person about whom personal data is retained in the database, and if the personal data in the database was data of special sensitivity – an amount of 8 new shekels for each person; If the amount of the aforementioned monetary sanction is less than 200,000 new shekels, the head of the authority may impose on the |

| | |
|---|---|
| (2) A database controller that has found that the database contains personal data that is not necessary according to Regulation 4(b) to the Regulations for the transfer of data from the European Economic Area and has not taken actions that ensure that it will not be possible to identify the data subject as referred to in Regulation 4(c), and the circumstances set forth in the aforementioned Regulation did not apply, and has not erased the aforementioned data at the earliest possible time under the circumstances, in violation of the provisions of Regulation 4(b) to the aforementioned Regulations, and this after receiving notice from the head of the authority under section 23ke(c) that its actions constitute a violation, and he did not cease the violation within the period instructed by the head of the authority. | database controller or the holder of the database a monetary sanction in the amount of 200,000 new shekels; Regarding items (1), (3) and (4) – the monetary sanction will be calculated based on the number of individual about whom the database controller did not delete personal data as required or did not provide them with notice as required under Regulation 3(c) or 6(a) or 6( b) to the Regulations for the Transfer of Data from the European Economic Area, as appropriate |
| (3) A database controller that received personal data about a person and did not notify him as required under Regulation 6(a) to the Regulations for the Transfer of Data from the European Economic Area, and none of the circumstances set forth in Regulation 6(c) to the aforementioned Regulations applied, in violation of the aforementioned Regulation 6(a), and this after receiving a notice from the head of the authority under section 23ke(c) that its actions constitute a violation, and it did not cease the violation within the period instructed by the head of the authority. | |
| (4) A database controller who sought to transfer the personal data it received to a third party and did not provide notice to the data subject as required under Regulation 6(b) to the Regulations for the Transfer of Data from the European Economic Area, and none of the circumstances set forth in Regulation 6(c) of the aforementioned Regulations applied, in violation of the aforementioned Regulation 6(b), and this after receiving notice from the head of the authority under section 23ke(c) that its actions constitute a violation, and it did not cease the violation within the period instructed by the head of the authority. | |

**Schedule 5**

(Section 23la)

**Reduced Amounts Regarding a Monetary Sanction**

1. Definitions

In this schedule –

"Turnover Certificate" – as specified below, as applicable:

(1) Regarding a violator who is required by law to appoint an auditor under the Companies Law, 5759-1999 – a certificate issued by the auditor;

(2) Regarding a violator who is a cooperative society – a certificate issued by a person who audited the accounts of the cooperative society under section 20 of the Cooperative Societies Ordinance;

(3) Regarding any other violator – a certificate issued by a certified public accountant or a tax advisor representing the violator, that the amount of Turnover presented by the violator corresponds to the amount stated in a document submitted to the Israel Tax Authority or the National Insurance Institute under the law; for this purpose, "tax advisor representing" – as defined in the Regulation of Representation by Tax Consultants Law 5765-2005;

"Turnover" – the turnover of a dealer as defined in the Value Added Tax Law, 5736-1975; Regarding a non-profit organization as defined in that Law – turnover as defined in schedule 2 to the Associations Law, 5740-1980, and with respect to a public body that is not one of the aforementioned – the annual budget of that public body;

"Micro-enterprise" – a violator whose turnover in the year preceding the date of the breach did not exceed 4 million new shekels;

"Small enterprise" – a violator, other than a micro-enterprise, whose turnover in the year preceding the date of the breach exceeded 4 million new shekels and did not exceed 10 million new shekels.

2. Reduction due to The Violator's Conduct

The head of the authority shall reduce the amount of the monetary sanction for a violator by the percentages specified below, if one or more of the following circumstances exist:

(1) In the five years preceding the breach of the provision for which a monetary sanction is imposed on the violator, no monetary sanction or administrative enforcement measure was imposed on him under chapters B to E of chapter D'3 for breach of the same provision – by 20%; and if in the three years preceding the violation no monetary sanction or administrative enforcement measure as aforesaid was imposed on the violator – by 10%;

(2) The violator ceased the violation on his own initiative and reported it to the head of the authority – by 30%;

(3) the violator took measures to prevent recurrence of the violation and to reduce the damage, to the satisfaction of the head of the authority – by 20%;

(4) The violator is obligated to appoint a privacy protection officer only under section 17b1(a)(3) and (4), and appointed such an officer before the notice of intention to impose a sanction was delivered – by 10%; such a reduction shall apply as long as the minister of justice has not, with the approval of the constitution committee, made an order under section 23ko(d)(1)(g).

3. Reduction due to Payment or Other Compensation Paid

the head of the authority may reduce the amount of the monetary sanction for a violator due to compensation paid or awarded against the violator for the same violations – by a percentage not exceeding 30%.

4. Reduction due to Personal Circumstances

If the head of the authority considers, with respect to a violator who is an individual, that the violation was caused by personal circumstances justifying a reduction of the monetary sanction or that severe personal circumstances exist justifying not exhausting the law with the violator, he may reduce the amount of the monetary sanction imposed on the violator by 20%.

5. Reduction due to Several Circumstances

If several circumstances as mentioned in sections 2, 3 and 4 exist with respect to a violator, the head of the authority may reduce the amount of the monetary sanction imposed on him by the percentages specified next to those circumstances, cumulatively, provided that the cumulative reduction percentage does not exceed 70% of the amount of the monetary sanction.

6. Reduction for a Micro or Small Enterprise

If the head of the authority finds, at the request of the violator, that the violator is a micro or small enterprise, as the case may be, he shall reduce the amounts of the monetary sanction imposed on him, whether or not they were reduced under section 2, 3 or 4, so that the amount of the sanction for violations under each of the paragraphs listed below shall not exceed the amount specified beside them:

(1) Regarding violations listed in section 23kf(a) and (b), in items (6) to (8), (11) to (14) and (25) to (28) of schedule 3, and item (1) in Part A of the Fourth schedule – for a micro-enterprise – 20,000 new shekels, and for a small enterprise – 40,000 new shekels.

(2) Regarding violations listed in section 23kf(c) to (f), in items (1) to (5), (9) and (10), (15) to (24) and (29) of schedule 3, in items (2) to (4) of Part A of the Fourth schedule and in Part B of that schedule – for a micro-enterprise –50,000 new shekels, and for a small enterprise – 100,000 new shekels.

(3) Regarding violations listed in section 23kf(z) – for a micro-enterprise –70,000 new shekels, and for a small enterprise –140,000 new shekels

If a violator who is a micro-enterprise or a small enterprise violates several provisions under paragraphs (1) to (3), the violator shall not bear an amount exceeding the highest monetary sanction.

7. Reduction due to Consideration of Turnover

(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 under section 2, 3, 4, or 6 or not reduced as aforesaid, exceeds 5% of the violator's turnover, the head of the authority shall reduce the amount of the monetary sanction to 5% of the violator's turnover; however, for a business with no 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 may be imposed under section 6 regarding a micro-business.

(b) A violator requesting a reduction of the amount of the monetary sanction under section 6 or this section shall submit to the head of the authority a turnover certificate within 30 days from the date of delivery of the notice of intent to impose a sanction