-Unofficial Translation-

Privacy Protection Law, 5741-1981

The Privacy Protection Law, 5741-1981

CHAPTER A: Infringement of Privacy

1. Prohibition of Infringement of Privacy

No person shall infringe the privacy of another without his consent.

2. What is a Privacy Infringement

Infringement of privacy is any of the following:

(1) Spying on or trailing a person in a manner likely to harass him, or any other harassment;

(2) Listening-in prohibited under any Law;

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

(4) Publishing a person's photograph under such circumstances that the publication is likely to humiliate him or bring him into contempt;

(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 or using, without permission from the addressee or writer, the contents of a letter or any other writing not intended for publication, unless the writing is of historical value or fifteen years have passed since the time of writing. In this Article "writing" - including electronic message as defined in Electronic Signature Law, 5761 – 2001;

(6) Using a person's name, appellation, picture or voice for profit;

(7) Infringing a duty of secrecy laid down by law in respect of a person's private affairs;

(8) Infringing a duty of secrecy laid down by express or implicit agreement in respect of a person's private affairs;

(9) Using, or passing on to another, information on a person's private affairs for a purpose other than for which it was given;

(10) Publishing or delivering anything obtained by way of an infringement of privacy under subsections (1) to (7) or (9);

(11) Publishing any matter relating to a person's intimate life, including his sexual history, state of health or conduct in the private domain.

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 infringement, unless one of the following applies:

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

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

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

(a) His spouse;

(b) All of his children;

(c) His parents;

(d) All of his siblings;

(4) The deceased had no family members listed in subsection (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 Article.

3. In This Law –

"data security" – the protection of the integrity of the data, or protection of the data from being processed, without lawful permission;

"person" – for the purpose of Articles 2, 13, 14, 15A, 17B, 17B1, 17B2, 17F, 23B, 23M(f), and 25, and for the purpose of the definitions of "direct mailing", "database", "biometric identifier", "personal data", and "data of special sensitivity" – excluding a corporation;

"database controller" - whoever 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, 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 Law on Adjudication of Interest and Indexing, 5721-1961;

"consent" – informed consent, explicit or implied;

"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 Law" – 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;

"Detention Law" – Criminal Procedure (Enforcement Powers – Detention) 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 by itself indicate additional personal data regarding the individuals whose names are included in it, provided that the owner of the collection or a corporation under the owner's control does not have another collection that includes other details about the same individuals;

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

"processor", for the purpose of a database – an external entity outside the database controller that is processing data on its behalf;

"personal data" – data item 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 by an identifier such as name, identification number, biometric identifier, location data, online identifier, or one or more data items 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 digital manner;
(5) Personal data about a person's ethnic origin;
(6) Personal data about a person's criminal record;
(7) Personal data about a person's political views or religious beliefs or worldview;
(8) Personal data which is a personality assessment conducted by a professional that, as part of their occupation, expresses an opinion on a person's personality, or 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, about a person, and data about a person's location that can give an indication on data under subsections (1) to (7) and (11);
(10) Personal data about a person's salary and financial activity;
(11) Personal data subject to confidentiality by law;
(12) Other personal data determined by the Minister of Justice, with the approval of the Constitution Committee, in Schedule 2, provided that such personal data is in a database in Israel that was transferred to it from outside the country's borders, and that in the jurisdiction from which it was transferred, special legal provisions apply to such personal data compared to the applicable law for other personal data.

"manager of a database" – the database controller, and for a public body as defined in 23 – the director general of the body that controls or possesses the database or person whom the aforesaid director authorized for this purpose;

"document" including output;

"inspector" – a person authorized in accordance with the provisions of Article 23I;

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

"system data" – data regarding the possession and management of personal data and of a database and their use, 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, provision, or granting access to it;

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

"publication" has the same meaning as in Article 2 of the Prohibition of Defamation Law, 5725-1965;

"photography" includes filming;

"Head of the Authority" – An individual appointed by the government to lead the Privacy Protection Authority and oversee 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 data in the database is identical to the source from which it was drawn, not having been changed, delivered or destroyed without lawful permission.

4. Privacy infringement – Civil Wrong

An infringement of privacy is a civil wrong, and the provisions of the Torts Ordinance (New Version) shall apply to it subject to the provisions of this Law.

5. Privacy Infringement – Criminal Offence

A person who willfully infringes the privacy of another in any of the ways stated in Articles 2(1), (3) to (7) and (9) to (11) is liable to imprisonment for a term of five years.

6. Trivial Act

No right to bring a civil or criminal action under this Law shall accrue though an infringement of no real significance.

CHAPTER B: Privacy Protection in Databases

7. (Revoked)

Subchapter A: Databases

8. Database Management and Lawful Processing of Personal Data

(a) In this Article, "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 in deviation from such authorization.

(d)

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

(2) If personal data was provided to a database controller by a different entity, and the controller did not and could not have known that the entity acted unlawfully, the database controller shall not be liable under this subsection for the processing of 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 minor violations of the law under the circumstances, and regarding personal data provided under subsection (2), even if the controller knew or should have known.

8A. Registration or Notification Obligation

(a) (1) A database must be registered if one of the following is applicable:

(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 Article 23, unless the database includes personal data only about the employees of the public body;

(2) A database controller shall not process personal data in a database that is subject to registration obligation and shall not permit another to process such data on its behalf, unless the database is registered in the registry; for this purpose, a database shall be deemed as registered if the database controller submitted a registration application in accordance with the provisions of Article 9 and the period mentioned in Article 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 he was convinced that the registration is not necessary for ensuring compliance with this law regarding the database; such 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 about them exceeds 100,000, in a database that is not subject to registration obligation under subsection (a)(1), the database controller shall notify the Authority, within 30 days of the aforesaid occurrence, of the identity, address and contact details of the controller, of the identity and contact details of the data protection officer – if an appointment thereof is required under Article 17B1, and will provide the Authority with a copy of the database definitions document that is required under the Regulations promulgated under Articles 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 data protection officer and their contact details, on any change requiring an update to the database definitions document in accordance with the Regulations under Articles 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 types of controllers from the notification obligation.

(c) The provisions of this Article shall not apply to a database that only contains data that was made public pursuant to lawful Authority or was made available for public access pursuant to lawful Authority.

9. Application for Registration

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

(b) An application for registration shall state –

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

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

(2) The purposes for which the database was established and the purposes for which the data are intended;

(3) The kinds of data that will be included in the database;

(4) Particulars on the transfer of data abroad;

(5) Particulars on receiving data, on a permanent basis, from a public body as defined in Article 23, the name of the public body delivering the data and the nature of the data delivered, except for particulars that are delivered with the consent of the persons as to whom the information relates.

(c) The Minister of Justice, with the approval of the Constitution Committee, may make regulations prescribing further particulars to be stated in the application for registration.

(d) The controller or possessor of a database shall notify the Head of the Authority of every change in any of the particulars specified in subsection (b) or in subsection (c) and of the discontinuance of the operation of the database.

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

(a) Where an application for registration of a database is submitted–

(1) The Head of the Authority shall register it in the registry, within 60 days from the day the application was submitted to him, unless he sees reasonable cause for believing that the database serves or is liable to serve illegal activities or as a cover for them, or that the personal data included within it was created received, accumulated or collected in violation of this Law or in violation of the provisions of any law; however, if the Head of the Authority requested additional data and details from the applicant, the time 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 a number of 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 pursuant to subsection (1) and shall not exercise his power pursuant to subsection (2), unless he has given the applicant an opportunity to be heard.

(b) (Revoked)

(b1) (Revoked)

(b2) Where the Head of the Authority notified the applicant of his refusal to register the database or of the suspension of the registration, the applicant shall not be allowed to process personal data in the database and shall not permit another to process personal data on its behalf, unless the court has determined otherwise.

(b3) The Head of the Authority shall delete the registration of a database from the registry, if the database controller notifies him that the data in the database has been destroyed or transferred to another registered database and does not exist anymore or that the database is no longer subject to the registration obligation and has verified the notice by affidavit.

(c) (Revoked) (d) (Revoked) (e) (Revoked)
(e1) (Revoked)

(f) Where the database controller or processor infringes any provision of this law or regulations thereunder, or fails to comply with a request made to it by the Head of the Authority, the Head of the Authority may suspend the registration for a period that he shall determine, 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 processor was given the opportunity to be heard.

(g) (Revoked)

10A. (Revoked)

11. Notice to accompany request for information

A request from a person to receive personal data for its processing in a database shall be accompanied by a notice indicating –

(1) Whether that person is under a legal obligation to provide that data or whether providing the data depends on his volition and consent and the consequence of lack of consent;
(2) The purpose for which the data is requested;

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

(3) To whom the personal data is to be delivered and the purposes of such delivery.

(4) The existence of the right of access to the personal data under Article 13 and the right to request the rectification of the personal data under Article 14.

12. Registry of Databases

(a) The Head of the Authority shall manage a register of databases, which shall be open for review by the public and shall enable to search its particulars.

(b) The register shall contain the particulars for registering the database under Article 9, except for the name of the data protection officer.

(c) Notwithstanding the provisions of subsections (a) and (b), in a database of a security Authority, the particulars stated in Article 9(b)(1A) and (3), (4), and (5) shall not be open to review by the public.

13. Right of Access to Personal Data

(a) Every person is entitled to access, either by himself or through a representative authorized by him in writing or his guardian, any personal data about him kept in a database.

(b) The database controller shall enable, at the request of a person referred to in subsection (a) (hereinafter – person making the request) access to the personal data, in the Hebrew, Arabic or English language.

(c) The database controller may refuse to provide the person making the request personal data relating to his physical or mental health if, in its opinion, it is liable to severely harm the physical or mental health of the person making the request or endanger his life; in such case, the database controller shall provider the data to a physician or psychologist on behalf of the person making the request.

(c1) The provisions of this Article shall not require the provision of personal data in violation of a privilege prescribed by law, unless the person making the request is the person who is the beneficiary of the privilege.

In this subsection, "law" includes case law.

(d) The mode and conditions of, and the payment for, the exercise of the right of access to personal data shall be prescribed by regulations.

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

(1) To a database of a security Authority within the meaning of Article 19(c);

(1a) To a database of the Israel Prison Service;

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

(3) Where the security or foreign relations of the State or the provisions of any enactment require that personal data about any person not be disclosed to him;

(4) To any database, in respect of which the Minister of Justice, in consultation with the Minister of Defense or the Minister of Foreign Affairs, as the case may be, and with the approval of the Foreign Affairs and Security Committee of the Knesset, has determined that it contains information as to which the security or foreign relations of the State requires or require that it not be disclosed (such information hereinafter referred to as "secret information"), provided that a person wishing to access personal data about himself kept at any such database shall be entitled to access information other than secret information;

(5) To a database about investigations and law enforcement of an Authority empowered by law to investigate an offense, which the Minister of Justice determined by order, with the approval of the Constitution Committee.

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

13A. Access to Personal Data Not Held by the Database Controller

Without derogating from the provisions of Article 13 –

(1) The database controller who keeps it with another (in this Article - the processor) shall refer the person making the request to the processor, with its address, and order the processor, in writing, to enable the person making the request the access;
(2) Where the person making the request applies to the processor first, the processor shall inform him if he possesses personal data about him, and also the name and address of the database controller.

14. Rectification of Personal Data

(a) A person who, when accessing personal data about himself finds that it is not correct, not complete, not clear or not up to date may request the database controller or, if such controller is a non-resident, the processor thereof to rectify or delete the personal data.
(b) Where the database controller agrees to a request under subsection (a), he shall make the necessary changes in the personal data and shall notify them to every person who received the personal data from it within a period prescribed by regulations.
(c) Where the database controller refuses to comply with a request under subsection (a), he shall give notice to such effect, in the form and manner prescribed by regulations, to the person who made the request.
(d) A Processor is obligated to rectify the personal data if the database controller agreed to the requested rectification or if a court ordered that the rectification be made.

15. A Court Claim

A person requesting data may, in the form and manner prescribed by regulations, file an action to the Magistrate's Court against a refusal by the database controller to enable access under Article 13 or Article 13A and against a notice of refusal under Article 14(c).

15A. Exemplary Damages

(a) If a database controller or a processor violate 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 Article – exemplary damages) of up to 10,000 NIS:

(1) Regarding a database controller – if the database is subject to the registration obligation under Article 8A – that controller processed personal data in a non-registered database, in violation of the provisions of the aforesaid Article, provided that the personal data subject demanded the registration of the database, and 90 days have passed since the day of his demand;

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

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

(4) Granted a request to rectify or delete personal data that is not correct, not complete, not clear, or not up to date, but did not make the necessary amendments to the personal data in its possession or did not notify of the amendments to everyone who received the personal data from it within the period of time prescribed by the regulations under Article 14(b), in violation of the provision of that Article;

(5) Did not notify the person who requested to rectify or delete personal data about him, that is not correct, not complete, not clear, or not up to date, of his refusal, in the manner and form prescribed by the regulations under Article 14(c), in violation of the provision of that Article;

(6) Regarding a database controller – did not notify the Head of the Authority about the regular reception of personal data, stored in a database in accordance with Article 23D(c), provided that the personal data subject demanded such notification from the controller, and 30 days have passed since his request.

(b) In determining the amount of exemplary damages, the court shall consider, *inter alia*, 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 payments imposed on the violator for the same violations.

(c) Nothing in this Article shall derogate from the possibility to conduct a criminal proceeding if the violation also constitutes a criminal offense, derogate from the possibility of using the powers under chapter D3, or derogate from the plaintiff's right to claim any other remedy under the Torts Ordinance [New Version], for the same violation; however, a person shall not receive exemplary damages in accordance with this Article more than once for the same act or omission.

16. Confidentiality

No person shall disclose any personal data obtained by him by virtue of his functions as an employee, manager or processor of a database save for the purpose of carrying out his work or implementing the Law or under a court order in connection with a legal proceeding; where the request is made before a proceeding has been initiated, it shall be heard by the Magistrate's Court. A person who infringes the provisions of this Article shall be liable to imprisonment for a term of five years.

17. Responsibility for Data Security

(a) The database controller and the processor 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 make regulations regarding the responsibility for data security set forth in subsection (a) and Article 17B(b), including its scope and the obligations included therein, as well as regarding the methods of securing the data, *inter alia*, on the following matters:

(a) Physical protection and the protection of logs in the database;

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

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

(3) Regulations under subsection (1) which will apply to entities listed in items 2 and 3 of the first Schedule to the Regulation of Security in Public Bodies Law will be enacted also in consultation with the Minister of Defense.

17A. (Revoked)

17B. Data Security Officer

(a) The bodies set forth below shall appoint a person with the appropriate qualifications to be in charge of the data security officer (hereinafter – data security officer):

(1) A controller of five databases subject to the registration or notification obligation under Article 8A or a processor of five such databases;

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

(3) A bank, an insurance company, a company involved in rating or evaluating credit.

(b) Without derogating from the provisions of Article 17, the data security officer shall be responsible for the data security in the databases kept in the possession of the bodies referred to in subsection (a).

(c) A person who has been convicted of an offense involving moral turpitude or an offense under this Law shall not be appointed as a data security officer.

17B1. Obligation to Appoint a Data Protection Officer

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

(1) A database controller that is a public body as defined in Article 23 or a processor of such a database, except for a security body as defined in Article 23K;

(2) A database controller whose 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;

(3) A database controller or processor whose core activities consist of data processing operations or involve such operations, which, given their nature, scope, or purpose, require regular and systematic monitoring of individuals, including tracking or systematic monitoring of a person's behavior, location, or activities on a significant scale, including but not limited to, an authorized provider who provides mobile radio telephone services under the Telecommunications Law (Telecommunications and Broadcasting) 5742-1982, and an online search service provider or anyone whose main occupation involves such actions;

(4) A database controller or processor whose main activity includes processing data of special sensitivity on a significant scale, including but not limited to, 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 as defined in the National Health Insurance Law, 5754-1994.

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

17B2. Roles of the Data Protection Officer

(a) The data protection officer shall act to ensure compliance with the provisions of this Law by the database controller or processor, and to promote the protection of privacy and data security in the databases, and *inter alia* -

(1) Serve as a professional Authority and central source of knowledge, 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 regarding databases, ensure its execution by the database controller or processor, report his findings to the management of the entity in which he performs his role, and make suggestions for rectifying deficiencies;

(3) Ensure the existence of a data security procedure and the database definition document, which are required to be prepared under the regulations in accordance with Articles 17(b) and 36, which will be brought to the approval of 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 access personal data or rectify it; the contact details of the data 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 processor, as applicable, shall provide the data protection officer with the conditions and resources required to properly perform his duties and shall ensure that the data protection officer is properly involved in all matters related to data protection law.

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

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

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

(b) The data protection officer can be someone who is not an employee of the entity in which he performs his role.

(c) The data protection officer shall not hold another position and shall not report to a person in the entity in which he performs his role or in another entity, if holding such 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 processor 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 mailing services.

17E. Indication of Data Sources

A database controller or processor shall not process personal data in a database used for direct mailing services, unless he has a record indicating the source from which he received every collection of data used for the database, and the date it was received, and to whom each said collection of data was provided.

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

(a) Every contact by direct mailing shall include in a clear and conspicuous manner–

(1) Mention that the contact is direct mailing, indicating the registration number of the database being used for direct-mailing services as stated in the Register of databases;

(2) Notice of the right of the recipient of the contact to be removed from the database as referred to in subsection (b); along with the address which he should contact for this purpose;

(3) The identity of the database controller containing the personal data based on which the contact was made, and the sources from which the database controller received this data.

(b) Every person is entitled to demand, in writing, of the controller of the database used for direct mailing that the personal data relating to him be deleted from the database.

(c) Every person is entitled to demand, in writing, of the controller of the database used for direct-mailing services or of the controller of the database containing the data based on which the contact was made, that the personal data relating to him not be delivered to a person, to a type of persons or to specific persons, for either a limited period of time or permanently.

(d) Where a person informed the database controller of his demand as specified in subsections (b) or (c), the database controller shall act in accordance with the demand and notify the person, in writing, that he acted accordingly.

(e) Where the database controller did not give notice as specified in subsection (d) within 30 days from the day of 12 receipt of the demand, the person whom the data are about may apply to the Magistrate's Court in the manner prescribed by regulations, to order the database controller to act as specified.

(f) The rights under this Article of a deceased person recorded in a database are also given to his spouse, child, parent, or siblings.

17G. (Revoked)

17H. No Applicability to a Public Body

This part shall not apply to a public body within the meaning of Article 23(1) in carrying out its functions under law.

17I. Reservation of Laws

The provisions of this part 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 civil servant unless otherwise established 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 Article 9(a) of the Freedom of Information Law shall not be published, and the Authority may choose not to publish details that constitute data that a public Authority is not required to disclose under Article 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 a database controller or processor, or someone who is about to become one of these, the Authority shall provide a preliminary opinion regarding the compliance of the database with the requirements of this Law or 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 the necessary facts for the issuance of the opinion, along with the relevant documents.

(c) A preliminary opinion shall be given within 60 days from the date of receipt of the request under subsection (b) or from the date on which the relevant documents have been provided, whichever is later; the Head of the Authority may defer the date, under special circumstances; if the Authority has decided 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 details that may lead to his identification.

(e) The Head of the Authority shall determine a procedure, which shall be published on the Authority's website, regarding methods to submit a request for a preliminary opinion and circumstances in which an opinion shall not be given, pertaining to 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 case law precedent;

(2) A request whose scope and implications are limited to the requester's matter in relation 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 unclean hands;

(5) A request relating to pending proceedings, including supervision, inquiry, or criminal enforcement, 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 Article - 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, *inter alia*, the following information, categorized by governmental ministries, other public bodies, and private entities:

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

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

(3) The number of databases required to be registered under Article 8A(a) that were given exemption from the registration obligation;

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

(5) The number of notifications about databases submitted to the Privacy Protection Authority under Article 8A(b) and the number of database controllers or processors of the said databases, that supervision or administrative inquiry in their regard, were conducted in the year following the submission of the notification;

(6) The number of complaints submitted to the Authority against database controllers or processors of databases, regarding violations under this Law;

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

(8) The number of administrative inquiry proceedings initiated under Article 23JB(a), and in how many of them it was decided to conduct an investigation instead of an inquiry proceeding, under Article 23IG(b);

(9) The number of search and seizure warrants, or computer material access warrants requested from the court under Article 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 Article 23JH(h), and how many of them were found to be justified;

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

(12) The number of administrative notices issued under Article 23LF, and in regards to how many of them a request to cancel was submitted under Article 23LG, and what were the outcomes of the requests;

(13) The number of cases in which a notification on the possibility of submitting a letter of undertaking and making a deposit was given, instead of imposing a monetary sanction under Article 23LI, and in how many cases the violator submitted a letter of undertaking and made a deposit under Article 23M(c);

(14) The sum of the monetary sanctions imposed under Article 23KF, the average amount of a monetary sanction imposed, the highest monetary sanction imposed, and the lowest monetary sanction imposed;

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

(16) The number of cases in which a notice of intent to impose a monetary sanction was issued, and no monetary sanction was imposed, and the reasons for not imposing;

(17) The number of cases in which the monetary sanction was reduced under Article 23LA and Schedule 5, in how many cases the sanction was reduced due to exceeding the maximum permissible percentage of the entity's turnover, in how many cases due to exceeding the cap for a small or micro enterprise under the same Schedule, and in how cases due to the appointment of a data protection officer in the entities listed in Articles 17B1(a)(3)-(4);

(18) The number of repeated violations that occurred, how many of them occurred after an administrative notice was issued under Article 23LF, and how many of them occurred after the submission of a letter of undertaking and making a deposit under Article 23M;

(19) The number of repeated violations that occurred;

(20) The number of appeals filed against the Head of the Authority's decision to impose a monetary sanction, administrative notice, or a letter of undertaking and a deposit under chapter D3, in how many of them the execution of the decision was stayed, and in how many of them the appeal was granted;

(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 under Article 23MF;

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

(23) Data on the criminal enforcement carried out by the Authority, *inter alia*, the number of investigations initiated by an investigator, the number of indictments filed following these investigations, categorized according to the offenses, in how many of them the proceedings ended in conviction, and what was the punishment in each case;

(24) The number of requests for the approval of the exercise of powers by the Head of the Authority, an inspector, or an investigator submitted to the Chair of the Central Election Committee or the Chair of the Regional Election Committee, as applicable, under Article 23NI; how many of them were granted, and in how many of them conditions were established.

(c) To the 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 exemplary damages under Article 15A and the case numbers of these lawsuits, according to the information provided to him by the Court Administration.

CHAPTER C: Defenses

18. What are Defenses

In any criminal, civil or administrative proceeding for an infringement of privacy, it shall be a good defense if one of the following occurs:

(1) The infringement was committed by way of a publication protected under Article 13 of the Prohibition of Defamation Law, 5725-1965;

(2) The defendant or accused committed the infringement in good faith and in one of the following circumstances:

(a) He did not know and need not have known that an infringement of privacy might occur;

(b) The infringement was committed in circumstances in which the infringer was under a legal, moral, social or professional obligation to commit it;

(c) The infringement was committed in defense of a legitimate personal interest of the infringer;

(d) The infringement was committed in the lawful pursuit of the infringer's occupation and in the ordinary course of its work, provided that it was not committed by way of publication;

(e) The infringement was committed by way of taking a photograph, or of publishing a photograph taken, in the public domain, and the injured party appears in it accidentally;

(f) The infringement was committed by way of a publication protected under subsections (4) to (11) of Article 15 of the Prohibition of Defamation Law, 5725-1965;

(3) The infringement involved a public interest justifying it in the circumstances of the case, provided that, if the infringement was committed by way of publication, the publication was not untruthful.

19. Exemption

(a) No person shall bear responsibility under this Law for an act which he is empowered to do by law.

(b) A security authority or a person employed by it or acting on its behalf shall bear no responsibility under this Law for an infringement reasonably committed within the scope of their functions and for the purpose of carrying them out.

(c) For the purposes of this Article, "security authority" means any of the following:

(1) The Israel Police;

(2) The Intelligence Branch of the General Staff, and the Military Police, of the Israel Defense Forces;

(3) The Israeli Security Agency;

(4) The Intelligence and Special Duties Agency;
(5) The Witness Protection Authority.

20. Burden of Proof

(a) Where the accused or defendant proves that he committed the infringement of privacy under any of the circumstances referred to in Article 18(2) and that it did not exceed the limits reasonable under those circumstances, he shall be presumed to have committed it in good faith.

(b) The accused or defendant shall be presumed not to have committed the infringement of privacy in good faith if in committing it he knowingly went further than was reasonably necessary for the purposes of the matters protected by Article 18(2).

(c) An accused person or defendant who claims to have a defense provided by Article 18(2)(b) or (d) shall be presumed not to have infringed privacy in good faith if he infringed it in violation of the rules or principles of professional ethics applying to him by law or accepted by members of the profession to which he belongs; however, this presumption will not apply if the infringement was caused in circumstances that the accused person or defendant acted according to a legal duty that was imposed on him.

21. Rebuttal of Defense Claims

Where the accused or defendant produces evidence or himself testifies to prove one of the defense pleas provided by this Law, the prosecutor or plaintiff may produce rebutting evidence. This provision shall not derogate from the power of the court under any law to permit the production of evidence by the parties.

22. Mitigating Factors

In passing sentence or awarding compensation, the court may also take the following into account in favor of the accused or defendant:

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

(2) That he did not intend to commit an infringement;

(3) If the infringement was committed by way of publication – that he has apologized and has taken steps for the discontinuance of the sale or distribution of copies of the publication containing the infringement, provided that the apology was published in the same place and in the same dimensions and manner in which the infringing matter had been published and was unqualified.

CHAPTER D: Providing Information or Data by Public Bodies

23. In this chapter

"Public Body" means:

(1) A Government Department and any other State institution, a local authority and any other body carrying out public functions under any law;

(2) A body designated by the Minister of Justice, by order, with the approval of the Constitution Committee, provided that the order shall prescribe the categories of data and data items which the body may provide and receive.

23A (revoked)

23B. Prohibition on Providing Data

(a) The provision of personal data by a public body is prohibited unless it has been published by lawful authority, or the person to whom it relates has consented to it being provided.

(b) The provisions of this Article shall not prevent a security authority, within the meaning of Article 19, from receiving or providing personal data for the purpose of carrying out its functions, provided that its provision or receipt is not prohibited by any enactment.

23C. Exception to the Prohibition

Notwithstanding the provisions of Article 23B, the provision of personal data, unless prohibited by any enactment or by the principles of professional ethics, is permitted –

(1) Between public bodies, if:

(a) The provision of the personal data takes place within the framework of the powers or functions of the data provider and is required for the purpose of implementing any enactment or for any purpose within the framework of the powers or functions of the data receiver, or

(b) The personal data is provided to a public body permitted by law to demand it from any other source;

(2) From a public body to a Government Department or other State institution, or between such Departments or institutions as aforesaid, if the provision of the personal data is required for the purpose of implementing any enactment or for any purpose within the framework of the powers or functions of the data receiver; provided that no personal data shall be provided as aforesaid if it had been given on condition that it not be provided to another.

23D. Obligations of a Public Body

(a) A public body which regularly provides personal data under Article 23C shall indicate such fact in every request for data made in accordance with the Law.

(b) A public body which provides Personal data under Article 23C shall keep a record of the personal data provided.

(c) Where a public body receives personal data under Article 23C on a regular basis and such personal data is stored in a database, it shall notify the Head of the Authority of such fact, and such fact shall be included in the particulars of the registry under Article 12.

(d) A public body which receives personal data under Article 23C shall only make use of it within the framework of its powers or functions.

(e) For the purposes of the duty of confidentiality under any law, any personal data provided to a public body by virtue of this Law shall be treated like personal data obtained by that body from any other sources and, in addition, all the provisions applying to the providing body shall apply to the receiving body

23E. Excessive Personal Data

(a) Where any personal data permitted to be provided under Article 23B or 23C is stored in a file with any other personal data (hereinafter referred to as "excess personal data"), the providing body may provide the requested personal data to the receiving body together with the excess personal data.

(b) Excess personal data may be provided under subsection (a) only upon establishing procedures preventing any use being made thereof. Such procedures shall be prescribed by regulations. As long as they have not been so prescribed, the requesting body shall establish procedures in writing and shall submit a copy thereof to the providing body upon request.

23F. Permitted Provision Does Not Infringe Privacy

The provision of personal data permitted under this Law shall not constitute an infringement of privacy and the provisions of Articles 2 and 8 shall not apply thereto.

23G. Regulations on The Provision of Personal Data

The Minister of Justice may, with the approval of the Constitution Committee, make regulations as to procedure for the provision of 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 authorize an inspector from civil servants, who will hold 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 authorization for reasons of public safety, including due to his criminal record;

(2) He received appropriate training regarding the powers he will hold under this Law and has met additional qualification conditions if prescribed, as determined by the Minister of Justice, with the agreement of the Minister of National Security, and regarding the exercise of the powers to access computer material or copy thereof under Article 23JD – his position qualifies him to perform such activities;

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

(b) The inspector's authorization under this Article shall be by 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 authorization under subsection (b) shall be published in the Official Gazette and on the Privacy Protection Authority's website.

Subchapter B: Supervisory Powers

23J. Inspector's Powers

(a) For the supervision of carrying out of provisions under chapters B, D, and E, and for the supervision of carrying out of provisions that the Head of the Authority is authorized to order the cessation of their violation under Article 23KH, an inspector authorized under the provisions of subchapter A (hereinafter – inspector) may:

(1) Require any person he believes to be a concerned party to provide his name and address and present an identity card or other official document that identifies him;

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

(3) Require any person concerned to present him or provide him with a copy of computer material containing system data or sample data; sample data under this Article will not be collected in excess to what is necessary to achieve the supervisory purposes;

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

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

(c) The Head of the Authority shall delete system data or sample data provided or collected under subsection (a)(3) when they are no longer reasonably required for the continuation of the supervisory proceedings, and no later than three years from the date of the provision or collection of the data, and regarding system data – within seven years unless the data is required for proceedings under subchapter B or C of this chapter, under chapter D3, or under chapter D4.

23JA. Inspector Identification

An inspector shall 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 holds 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 that the Head of the Authority is authorized to order the cessation of under Article 23KE, or a provision under this Law mentioned in Article 23KF, he may initiate an administrative inquiry proceeding regarding the violation and exercise the powers under Article 23J for that matter.

(b) In an administrative inquiry proceeding under subsection (a), the identification requirement under Article 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 shall fulfill said obligation as soon as possible.

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

Before exercising his powers under this subchapter, the inspector shall notify the person that an administrative inquiry proceeding concerning the database is being conducted and the nature of the inquiry; once notified, the person must answer the questions asked, but the answers given will not be used as evidence in a criminal proceeding against him if he had no obligation to answer them if he was asked under Article 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 authorized to do so, has reasonable grounds to assume that a violation of a provision under this Law mentioned in Article 23JB(a) has been committed, he may request a search and seizure order or an order for access to computer material under Articles 23(1), 23A, and 24 of the Arrest and Search Ordinance, and carry them out 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 proceeding shall be used solely for the purpose for which it was collected, and shall not be used as evidence in a criminal proceeding.

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

The provisions of Articles 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 computer material or copying thereof under this subchapter, with the necessary modifications, and the following changes: the powers granted to a police officer will apply to an inspector, and the powers granted to an Officer will apply to the Head of the Authority or an inspector authorized by the Head of the Authority.

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

(a) If the Head of the Authority has reasonable grounds to suspect that an act or omission (in this chapter – act) that can lead to a criminal investigation under subchapter A of chapter D4 or an administrative inquiry under this subchapter, the Head of the Authority shall decide on the conducting of an investigation or an administrative inquiry; the Head of the Authority's decision 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 act;

(3) The enforcement policy of the Authority.

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

(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; for the implementation of the plan, the Head of the Authority may be assisted by a non-civil servant in carrying out these activities (in this Article – assisting party):

(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, while the response and communication will be conducted with a non-civil servant and that the supervised entity will be entitled to contact a civil servant whose name and contact details will be specified in the request;

(2) Receiving 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 subsection (2), according to criteria determined by the Head of the Authority in a procedure;

(4) Contacting the supervised entity for supplementary information or update on the need for clarifications regarding the answers to 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 request submitted by a supervised entity in regards to a response to the questionnaire or the submission of documents, in accordance with the Authority's guidelines;

(7) Providing answers to the supervised entity on technical issues.

(b) In performing the actions, the assisting party shall act in accordance with the guidelines 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 party shall not perform an action requiring entry to a place under Article 23J(a)(4).

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

23JH. Assistance from an External Expert

(a) For the supervision of fulfillment of the provisions under chapters B, D, and E and for the exercise of his powers under subchapters B and C, and chapter D3, the Head of the Authority may be assisted by a person who is not a civil servant, and who has been granted authorization according to subsection (c) (in this Law — an external expert), 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, in accordance with his guidance and instructions and under his supervision; an 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 appoint a person who meets all the following as an external expert:

(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 be appointed as an external expert.

(d) The Head of the Authority may refuse to appoint as an external expert a person against whom criminal proceedings are pending for an offense which, due to its nature, severity or circumstances, makes him unfit to be appointed as an external expert.

(e) (1) No one shall be appointed as an external expert or serve as an external expert 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 in a conflict of interest as mentioned in subsections (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 such requirement is approved in advance by an inspector, and he may accompany an inspector entering a premise in accordance with Article 23J(a)(4).

(g) An external expert who receives data in accordance with this Article in the course 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 any other statute or by a court order.

(h) Anyone who 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 to be justified, he shall notify so to the applicant and the external expert, along with his decision; if the Head of the Authority finds the complaint to be 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 the provisions applicable to public servant laws in the Penal Law, 5737-1977, and the Public Service (Gifts) Law, 5749-1979;

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

(j) A notice of appointment as an external expert and an updated list of external experts shall be published on the Authority's website.

(k) In this Article—

"family member" – spouse, parent, grandparent, son or daughter and their spouses, siblings and their children, father-in-law, 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 a vote, or dealing with the subject outside a discussion;

"conflict of interest" of an external expert – a conflict of interest between the fulfillment of his duties and a personal interest or another 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 subsection (2) are an interested party in;

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

Subchapter E: Supervision and Administrative Inquiry in Bodies Under the Regulation of Security in Public Bodies Law

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

The manner of exercising the powers in accordance with subsections B and C regarding the bodies listed in the fifth Schedule of the Regulation of Security in Public Bodies Law, shall be determined in a procedure established by 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 the 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) Israel Police;

(2) Israel Defense Forces;

(3) Israeli Security Agency;

(4) Intelligence and Special Duties Agency;

(5) National Cyber Directorate;

(6) Witness Protection Authority;

(7) Israel Prison Service;

(8) 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 of the Regulation of Security in Public Bodies Law, and that the Minister of Defense notified the Minister of Justice about them;

(11) Other 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 Knesset's Constitution Committee and the Foreign Affairs and Defense Committee;

"Head of a Security Body", for the purposes of 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 D1 shall not apply to security agencies, and the supervision and administrative inquiry of security agencies shall be carried out in accordance with the provisions of this chapter;

(c) The Minister of Defense, with the consent of the Minister of Justice, may exclude from the publication in the Official Gazette of an order under in subsection (11) of the definition "security agency" in subsection (a), the name of an agency in respect of which the order was issued, for reasons of protecting national security; however, the full text of the order, that 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), in accordance with the qualification and training requirements determined 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's term shall be for no less than three years.

(c) The tenure of the internal inspector shall not be terminated and he shall not be removed from his position without consultation with the Head of the Authority.

(d) The internal inspector shall be an employee of the security agency and report directly to the Head of the security agency, or to a senior employee of the security agency who reports directly to the Head of the security agency and shall receive professional instructions from the Head of the Authority.

(e) The internal inspector shall not hold any additional position or engage in any additional occupation that may place him in potential 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 his 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 monitor their exercise, and *inter alia*:

(1) Prepare an annual work plan to be submitted for approval by the Head of the security agency and by 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 their cessation under Article 23KE and violation of any of the provisions under this Law listed in Article 23KF (in this Article – work plan);

(2) Examine the procedures of the security agency and its policy on privacy protection and its compliance with the provisions of the law and the security agency's policy on 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 their cessation under Article 23KE and violations of the provisions under this Law listed in Article23KF, 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 clearance provisions, as set out in Article 15 of the Israel Security Agency Law, 5762-2002, and the Compartmentalization rules applicable to the security agency, on the findings of the supervision and examination activities he 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 was implemented and on compliance with the provisions of the law that pertain to 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 vested in an inspector under subchapter B of chapter D1, and shall also be obligated to delete sample data as provided in Article 23J(c), with the necessary modifications.

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

(a) The Head of the Authority may order the internal inspector to take actions, including complementary or additional actions to those conducted by the internal inspector, or to correct deficiencies.

(b) The Head of the Authority may exercise the powers vested in him under chapter D3 if he finds that any of the violations that the Head of the Authority is authorized to order their cessation under Article 23KE, or of a provision listed in Article 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 aforementioned violations has occurred, and has 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 as determined by the Head of the Authority after consulting with the internal inspector, and the conditions of Article 23KG have been met.

(c) If the Head of the Authority deems that the findings under subsection (a) or (b) raise suspicion that an offense has been committed under this Law, or that he has otherwise become aware of such an offense, an investigator shall have the enforcement powers under Article 23NA, unless there was another investigative authority authorized by law to investigate offenses in that security agency; for the purposes of this Article, “other investigative authority” – other than the Israel Police.

(d) An investigator or the Head of the Authority shall not use their powers under this chapter with regard to a security agency unless he has undergone security clearance as set out in Article 15 of the Israel Security Agency Law, 5762-2002.

CHAPTER D3: 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 processor has used information about a person's private affairs in a database for a purpose other than for the purpose for which it was provided, contrary to the provisions of Article 2(9), or processed personal data in a database for a purpose that constitutes an infringement of privacy under Article 2, he may, after giving it an opportunity to present its arguments, notify it that its actions constitute a violation and order it to cease it in the manner and within a time period instructed by him.

(b) If the Head of the Authority finds that a database controller or a processor has processed personal data in a database that was created, received, accumulated or collected, contrary to the provisions of this Law or contrary to the provisions of any other law that regulates data processing, or has permitted another to process such personal data for him, contrary to Article 8(d), he may, after giving it an opportunity to present its arguments, notify it that its actions constitute a violation and order it to cease it in the manner and within a time period instructed by him.

(c) If the Head of the Authority finds that a database controller or a processor has processed data contrary to the provisions of the Regulations listed in part B of the fourth Schedule, he may, after giving it an opportunity to present its arguments, notify it that its actions constitute a violation and order it to cease such actions in the manner and within a period as instructed.

(d) If the Head of the Authority finds that one of the instances in subsections (1) to (4) below has occurred, he may, after giving the database controller or the processor who is required to appoint a data protection officer in accordance with Article 17B1(a), an opportunity to present its arguments, notify it that its actions constitute a violation, and order it to cease the violation and the manner in which it should be rectified; if the Minister of Justice has issued, with the approval of the Constitution Committee, an order under Article 23KF(d)(1)(g), the Head of the Authority may also issue such an order for the violation listed in subsection (5) below:

(1) The data protection officer has not been provided with the conditions and resources required to properly perform his duties, or he was not properly involved in all matters related to data protection laws, contrary to Article 17B2(b);

(2) The data protection officer does not report directly to the officials listed in Article 17B2(c);

(3) The data protection officer does not possess the required knowledge and skills under Article 17B3(a);

(4) The data protection officer holds another position or reports to a person in the entity in which he performs his role or in another entity, in a manner that may place him in a conflict of interest in the performance of his duties, contrary to Article 17B3(c);

(5) The database controller or the processor did not appoint a data protection officer, contrary to Article 17B1(a)(3) or (4).

(e) In an 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 deadline for its rectification;

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

(3) The violator's right to appeal within 45 days according to subsection (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 delivery of the order of cessation of the aforesaid violation;

(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 lodged, the violation of the Head of the Authority's order under this Article shall not be considered a violation until the court issues another decision.

(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 processor violated provisions under this Law, as specified below, the Head of the Authority may impose a monetary sanction on it 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 it with double the amount:

(1) Committed one of the following:

(a) Processed personal data in a database subject to the registration obligation without it being registered, contrary to the provisions of Article 8A(a);

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

(c) Did not notify the Head of the Authority of a change in the particulars specified in Article 9(b) or in the particulars determined in Article 9(c), contrary to the provisions of Article 9(d), except for a change in the address of the database controller;

(2) Did not notify the Head of the Authority of a database that is subject to the notification obligation under Article 8A(b) or failed to notify the Head of the Authority of a change in any of the details specified in that Article, contrary to the provisions of that Article;

(3) Processed personal data in a database used for direct mailing services, without the database being registered in the registry or without having direct mailing services as one of its registered purposes, contrary to the provisions of Article 17D;

(4) Failed to inform the Head of the Authority that he receives personal data on a regular basis in accordance with the provisions of Article 23C and the data is stored in a database, contrary to the provisions of Article 23D(c).

(b) If a database controller or a processor violated provisions of this Law, as specified below, the Head of the Authority may impose a monetary sanction on it 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 access the personal data about him, contrary to the provisions of Article 13;

(2) Made a change to the personal data in its possession without notifying everyone who received the data, contrary to the provisions of Article 14(b);

(3) Failed to notify the person who made the request of a refusal to rectify personal data held in a database in its possession or to delete it, contrary to the provisions of Article 14(c);

(4) Did not rectify personal data held in a database in its possession, contrary to the provisions of Article 14(d);

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

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

(c) (1) If a database controller or a processor violated provisions of this Law, as specified below, the Head of the Authority may impose a monetary sanction on it under the provisions of this chapter, in the amount of 50 new shekels multiplied by the number of individuals to whom the request or demand was made, as specified below, and if the request or demand was in relation to data of special sensitivity – in the amount of 100 new shekels multiplied by the number of individuals to whom it was made:

(a) Made a request to a person to receive personal data for its processing in a database, without providing him notice as required under Article 11;

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

(c) A database controller that has not indicated in a request for personal data, that he provides data on a regular basis in accordance with Article 23C, contrary the provisions of Article 23D(a);

(2) If the amount of the monetary sanction under subsection (1) is less than 30,000 new shekels, the Head of the Authority may impose on a database controller or processor a monetary sanction in the amount of 30,000 new shekels.

(d) (1) If a database controller or a processor violated the provisions of this law, as specified below, the Head of the Authority may impose a monetary sanction on it 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) Made a request to a person to receive personal data for its processing in a database, and the request was made to an unspecified group of individuals, without providing him notice as required under Article 11, contrary the provisions of that Article;

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

(c) Did not appoint a data protection officer, contrary to the provisions of Article 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 it received every collection of data used for the database, the date it was received and to whom each collection of data was provided, contrary to the provisions of Article 17E;

(e) A database controller that did not keep a record of the personal data it provided in accordance with Article 23C, contrary to the provisions of Article 23D(b);

(f) With regard to a database controller listed in Article 17B1(a)(1) or (2) – did not comply with the Head of the Authority's order to cease or rectify a violation, contrary to the provisions of Article 23KE(d);

(g) The Minister of Justice, with the approval of the Constitution Committee, may determine, by order, that the provisions of subsection (f) shall also apply to a database controller or processor listed in Article 17B1(a)(3) and (4);

(2) In a monetary sanction under subsections (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 subsections;

(3) If the amount of the monetary sanction under subsection (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 processor in the amount of 20,000 new shekels or 40,000 new shekels, as applicable.

(e) (1) If a database controller or a processor violated the provisions under this Law, as specified below, the Head of the Authority may impose a monetary sanction on it under the provisions of this chapter in the amount of 4 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 8 new shekels per person:

(a) Failed to comply with the Head of the Authority's order under Article 23KE(a) to cease the use of information on a person's private affairs in a database for a purpose other than for which it was given, contrary to the provisions of Article 2(9), or to cease the processing of personal data in a database for a purpose that constitutes an infringement of privacy under Article 2;

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

(c) Failed to comply with the Head of the Authority's order under Article 23KE(b) to cease the processing of personal data in a database that was created, received, accumulated or collected, contrary to the provisions of this Law or contrary to the provisions of any law that regulates data processing, or to cease allowing another to process such personal data for him;

(d) Processed personal data without authorization from the database controller, or in deviation from such authorization, contrary to the provisions of Article 8(c);

(e) A database controller that provided data from a public body, contrary to the provisions of Article 23B, without meeting the conditions of Article 23C;

(2) If the amount of the monetary sanction under subsection (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 processor.

(f) If a database controller or a processor processed personal data in a database not for the purpose that was established for it, contrary to the provisions of Article 8(b), in circumstances where such a purpose could have been lawfully established, the Head of the Authority may impose a monetary sanction on it under this chapter in the amount specified in detail (1) of the third Schedule.

(g) If a database controller or a processor failed to provide an inspector with a document or a copy of computer material, contrary to the provisions of Article 23J(a)(2) or (3), the Head of the Authority may impose a monetary sanction on it under this chapter in the amount of 300,000 new shekels.

(h) If a database controller or a processor violated any of the provisions of the Regulations established pursuant to Article 36, as specified in column A of the third Schedule, which are applicable to it, the Head of the Authority may impose a monetary sanction on it under this chapter in the amount specified in column B, column C, column D, or column E alongside that provision, as applicable, and if the database is a database to which the high level of security applies under the third Schedule, and that contains data about 1,000,000 individuals or more, the Head of the Authority may impose double the amount set forth in column E alongside that provision.

(i) (1) If a database controller or a processor violated any of the provisions of the Regulations established under Article 36, in the fourth Schedule, under column A of part A of that Schedule, the Head of the Authority may impose a monetary sanction on it under this chapter in the amount specified in column B alongside that provision;

(2) If a database controller or a processor did not comply with the Head of the Authority's order under Article 23KE(c) to cease the violation of the provisions of the Regulations listed in part B of the fourth Schedule, the Head of the Authority may impose a monetary sanction on it under this chapter, in the amount specified in column B alongside that provision in the fourth Schedule.

(j) (1) If the processor was issued a demand for payment due to a violation of a provision under subsection (h), the Head of the Authority shall notify the database controller of that database along with a copy of the demand for payment issued to the processor, and shall order the database controller to take actions to cease the violation by the processor, all within a time period as determined by the Head of the Authority;

(2) If the violation under subsection (1) was not ceased, and the database controller did not comply with the Head of the Authority's order regarding the cessation of the violation, the Head of the Authority may issue it a notice of intent to charge under Article 23KG due to that violation, and the provisions of this subchapter shall apply to the database controller regarding that violation, with the necessary modifications, as if it 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 processor for that violation.

23KG. Notice of Intent to 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 listed in Article 23KF (in this chapter – the violator), and he intends to impose a monetary sanction on it under that Article, he shall provide the violator with written notice of the intent to impose a monetary sanction on it (in this Law – notice of intent to charge).

(b) In the notice of intent to charge, the Head of the Authority shall indicate, *inter alia*, 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 time period for its payment;

(3) The right of the violator to present its arguments before the Head of the Authority under Article 23KH, and that the notice of intent to charge shall be deemed as a demand for payment if the violator does not exercise the said right, pursuant to Article 23KI(d);

(4) The power to increase the amount of the monetary sanction due to a continuous or repeated violation under Article 23L, and the rate of the increase.

23KH. Right to Argue

A violator to whom a notice of intent to charge has been provided under Article 23KG may present its arguments before the Head of the Authority, in writing or orally, as decided by the Head of the

Authority, regarding the intent to impose a monetary sanction on it and regarding its amount, within 45 days from the date of delivery of the notice; the Head of the Authority may extend the 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 Article 23KH, whether to impose a monetary sanction on the violator, and he may reduce the amount of the monetary sanction under Article 23LA.

(b) (b) If the Head of the Authority decides under subsection (a)–

(1) To impose a monetary sanction on the violator – he shall provide it with a demand, in writing, to pay the monetary sanction (in this chapter – a demand for payment), in which he specifies, *inter alia*, the amount of the updated monetary sanction and the time period for its payment, as well as the right of the violator to lodge an appeal within 45 days under Article 23ME;

(2) Not to impose a monetary sanction on the violator – he shall notify it 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 did not present its arguments under Article 23KH within the time period mentioned in that Article, the notice of intent to charge, at the end of that period, shall be deemed as a demand for payment delivered to the violator on the aforesaid date.

23L. Continuous Violation and Repeated Violation

(a) (1) In a continuous violation, the monetary sanction specified for that violation will be increased by one percent of the amount for each day of which the violation continues; for that matter, "continuous violation" means a violation of any of the provisions of this Law, as stated in Article 23KF, after the violator has been given a demand for payment due to a violation of that provision;

(2) If an appeal was lodged against the demand for payment decision, the time period until the court decides on the matter shall not be taken into account for the purposes of subsection (1), unless the court has determined 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 of this Law, as stated in Article 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 the cases, 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 its arguments before the Head of the Authority under Article 23KI(d) – on the date of delivery of the notice of intent to charge; if an appeal is filed to the court and the 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 applicable.

(b) The amounts determined in Article 23KF and the amounts set forth in the third, fourth and fifth Schedule shall be updated on January 1 of each year (in this subsection – the date of update), in accordance with the known rate of change in the index on the date of update compared with the known index on January 1 of 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 the delivery of the payment demand under Article 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 Law on Adjudication of Interest and Indexing, 5721-1961, shall apply with the necessary modifications.

23LE. Collection

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

Subchapter C: Administrative Notice

23LF. Administrative Notice

(a) If the Head of the Authority has reasonable grounds to believe that a person has violated any of the provisions of this Law, under Article 23KF, and circumstances determined by the Minister of justice have occurred, the Head of the Authority may, instead of imposing a monetary sanction on it under subchapter B, issue an administrative notice in accordance with the provisions of this subchapter.

(b) In an administrative notice, the Head of the Authority shall indicate the act constituting the violation, the circumstances of its commission, and the date of its commission, inform the violator that he must cease 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 monetary sanction, under Article 23LH, and shall also indicate the right of the violator to request the cancellation of the notice under Article 23LG.

23LG. Request to Cancel an Administrative Notice

(a) If an administrative notice is issued to the violator under Article 23LF, the violator may submit a written request to the Head of the Authority, within 45 days, to cancel the administrative notice for any of the following reasons:

(1) The violator did not commit the violation;

(2) The act committed by the violator, as specified in the administrative notice, 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 notice, under subsection (a), he may cancel the administrative notice or reject the request and leave the administrative notice as it is; The Head of the Authority's decision shall be given in writing and shall be issued to the violator with reasoning.

23LH. Continuous Violation and Repeated Violation After a Notice

(a) If an administrative notice is issued to the violator under this subchapter and the violator continues to violate the provision for which the notice was issued, the violation shall be deemed as a continuous violation, the provisions of Article 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 under Article 23KG, with the necessary modifications.

(b) If an administrative notice is issued to the violator under this subchapter and the violator repeats the violation of the provision for which the notice was issued, within two years from the date of delivery of the notice, the additional violation shall be deemed as a repeated violation under Article 23L(b), and the Head of the Authority shall provide the violator with a notice of intent to charge for the repeated violation, under Article 23KG, with the necessary modifications.

Subchapter D: Obligation to Refrain from Violation

23LI. Notice of The Possibility of Submitting a letter of undertaking and a deposit

If the Head of the Authority has reasonable grounds to believe that a person has violated any of the provisions of this Law, as provided in Article 23KF, and circumstances determined by the Minister of justice have occurred , the Head of the Authority may give the violator written notice of its possibility of submitting to the Head of the Authority a letter of undertaking and making a deposit in accordance with the provisions of this subchapter, instead of a monetary sanction that may be imposed on it under subchapter B.

23M. Terms of letter of undertaking and a deposit

(a) In the letter of undertaking, the violator shall commit to cease the violation of the provision as provided under Article 23LI and to refrain from further violation of that provision, for a time period determined by the Head of the Authority and beginning on the date of the submission of the letter of undertaking, 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 undertaking additional conditions that the violator must commit to and comply with during the undertaking period, in order to reduce the damage caused by the violation or prevent its recurrence.

(c) In addition to the letter of undertaking, the violator shall make a deposit to the Authority in the amount of the monetary sanction that the Head of the Authority was authorized to impose on the violator due to that violation, taking into account circumstances and considerations under 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 making a deposit under subsection (c) or reduce the amount of the deposit that the violator makes under that subsection.

23MA. Results of Submitting a Letter of letter of undertaking and making a deposit or non-Submission

(a) If the violator submits a letter of undertaking to the Head of the Authority and makes a deposit under this subchapter, within 45 days from the date of delivery of the notice under Article 23LI, no monetary sanction shall be imposed for that violation; if the violator does not submit a letter of undertaking to the Head of the Authority or does not make a deposit within the said period, the Head of the Authority shall provide it with a notice of intent to charge for that violation, under Article 23KG.

(b) The Head of the Authority may extend the time period under subsection (a), for special reasons to be recorded.

23MB. Violation of undertaking

(a) If the violator submits a letter of undertaking and makes a deposit in accordance with this subchapter and violates any of the terms of the undertaking, as specified in the following subsections, the provisions specified in those subsections shall apply, as applicable:

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

(a) The Head of the Authority shall provide the violator with a notice of intent to charge for the continuous or repeated violation, as applicable, in accordance with the provisions of Article 23KG, with the necessary modifications;

(b) If the Head of the Authority provides the violator with a demand for payment due to the continuous or repeated violation, as applicable, in accordance with the provisions of Article 23KI(b)(1) or the violator has not argued its claims before the Head of the Authority regarding that violation under Article 23KI(d), the Head of the Authority shall forfeit the deposit in addition to the imposition of the monetary sanction due to the continuous violation or repeated violation; if the Head of the Authority decided, under Article 23M(d), to exempt the violator from making a deposit or to reduce the amount of the deposit, he shall provide the violator with a payment demand under Article 23KI, which also includes the amount of the deposit for which the exemption was granted or the part reduced from the amount of the deposit, as applicable, with the addition of the 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 undertaking under Article 23M(b), the Head of the Authority shall forfeit the deposit, and if he decided, under Article 23M(d), to exempt the violator from making a deposit or to reduce the amount of the deposit, he shall provide the violator with a demand for payment under Article 23KI regarding the amount of the deposit for which the exemption was granted or with respect to the part that was reduced from the amount of the deposit, as applicable, with the addition of the 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 deposit or send a demand for payment under this subsection unless he has given the violator an opportunity to argue its claims, in writing, regarding the violation of such conditions.

(b) Regarding this chapter, the forfeiture of the deposit under this Article shall be deemed as the imposition of a monetary sanction on the violator due to the violation for which the deposit was made.

(c) If a condition of the terms of the undertaking under this Article is violated, and the violator repeats the violation of the provision for which he gave the letter of undertaking, the Head of the Authority shall not allow it to submit another letter of undertaking under this subchapter, for that same violation.

23MC. Return of deposit

If the violator complies with the terms of the letter of undertaking submitted under this subchapter, he will be refunded, at the end of the undertaking period, the deposit with the addition of the interest rate from the date of its submission 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 Article 23KF and of a violation under another law, no more than one monetary sanction shall be imposed.

23ME. Appeal, Stay of Execution, and Refund

(a) The imposition of an administrative enforcement measure under subchapters B to E can be appealed to the Magistrate's Court where the President of the Magistrate's Court resides, within 45 days from the date the notice of the measure.

(b) The lodging of an appeal against a decision of the Head of the Authority under subchapters B to E shall not stay 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, alter it, cancel it or make another decision in its place, 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 deposit has been made, to grant an appeal under 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 deposit, the amount paid or any part thereof that has been reduced or returned will be refunded, as applicable, with the addition of the interest rate from the date of its payment or making until the day of its return.

23MF. Publication

(a) If the Head of the Authority imposes a monetary sanction under this chapter, he shall publish the following details on the Privacy Protection Authority's website, 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 was reduced and the rates of reduction;

(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 Article shall not take place until the violator has been given an opportunity to argue its claims; the opportunity to argue claims under this subsection may be given to the violator as part of the right to argue under Article 23KH, provided that the Head of the Authority has notified the violator of its intention to publish its name, in the notice of intent to charge under Article 23KG.

(c) If an appeal is lodged against the decision of the Head of the Authority to impose a monetary sanction, the Head of the Authority shall, in the same manner published under subsection (a), publish the lodging of the appeal and its results.

(d) Despite the provisions of subsection (a)(6), the Head of the Authority -

(1) Shall not publish the name of a violator that is a corporation, if the Head of Authority was convinced that the violation is a minor violation under the circumstances, unless the publication is necessary to warn the individuals whose details are in the database;

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

(e) Despite the provisions of this Article, the Head of the Authority shall not publish details that constitute data that a public authority is prohibited from disclosing under Article 9(a) of the Freedom of Information Law, and he may also refrain from publishing details under this Article, which are information that a public authority is not obligated to provide under Article 9(b) of the said law.

(f) Publication under this Article 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 under this Article.

23MG. Maintaining Criminal Liability

(a) The payment of a monetary sanction, the provision of an administrative notice or the submission of a letter of undertaking and the making of a deposit under this chapter shall not detract from the criminal liability of a person for violating any of the provisions under this Law which constitute a criminal offense.

(b) Despite the provisions of subsection (a), if the violator has been provided with a notice of intent to charge, an administrative notice or a notice of the possibility of submitting a letter of undertaking and making a deposit, 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, under Article 23IG; If such new facts have been discovered and an indictment has been filed against the violator after the violator has paid a monetary sanction or made a deposit, the violator will be refunded the amount paid or the deposit, as applicable, with the addition of the interest rate and late payment fees from the date of payment of the amount or from the date of the making of the deposit, 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 him under subchapters B to E for the violation.

23MH. Delegation of Powers

The Head of the Authority may delegate his powers under subchapters B to E to a senior employee who reports directly to him and is responsible of monetary sanctions; notice of such delegation shall be published in the Official Gazette.

Subchapter F: Judicial Ban Order

23MI. A Judicial Ban on Processing Order 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 Article 2(9), 8(b), (c) or (d), 17 or 23B is being committed in a database, he may request an administrative court (in this Article – the court) to issue an order to the database controller or database processor, to stop processing activities that cause a violation or that there is a concern they will cause a violation (in this

Article – a ban order), and the court may also order the deletion of the personal data in the database in its entirety (in this Article – a deletion order).

(b) The court may issue an order under subsection (a), as requested or with modifications, if it was convinced that all of the following have occurred:

(1) There is reasonable ground 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 less infringing mean 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 Article shall be issued after the database controller has been given an opportunity to argue its claims before the court, and if the order is directed at the processor – the processor has been given the opportunity as well, to the extent possible, and in the appropriate manner under the circumstances;

(2) A ban order issued without the presence of a party as provided in subsection (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 time period of the order after the database controller or the processor, as applicable, has been given an opportunity to argue its claims.

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

(e) A proceeding under this Article shall be subject to 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 prescribe regulations regarding the procedures of a proceeding under this Article; until such regulations are prescribed, the provisions of the Citizenship Regulations (procedures for an application to revoke citizenship), 5777-2017, shall apply with the necessary modifications.

CHAPTER D4: Enforcement and Penal Powers Subchapter A: Enforcement Powers

23N. Appointment of Investigators

(a) The Head of the Authority may authorize an investigator from among civil servants, who will hold all or some of the powers under this Law, (hereinafter: an investigator), if all of the following apply to him:

(1) The Israeli Police announced, within three months of the Head of the Authority's request, that it does not object to his authorization for reasons of public safety, including due to his criminal record;

(2) He received appropriate training regarding the powers that he will hold under this law, and has met additional qualification conditions, if prescribed, as determined by the Minister of Justice with the agreement of the Minister of National Security, and regarding the exercise of powers to access computer material or copy thereof under 23NA(a)(3) – his position qualifies him to perform such activities;

(3) He has received appropriate training on privacy protection, as determined by the Minister of Justice.

(b) The investigator's authorization under this Article shall be by a certificate signed by the Head of the Authority, certifying his role as an investigator and his powers under this Law (hereinafter: an investigator's certificate).

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

23NA. Enforcement Powers

(a) If an investigator has reasonable grounds to suspect that an offense has been committed under Article 5, in the circumstances detailed in Article 2(9), and the suspicion is that the offense was committed regarding information about 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 subsection shall be subject to the provisions of Articles 2 and 3 of the Criminal Procedure Law (Testimony) and the provisions of the Criminal Procedure Law (Interrogation of Suspects), 5762-2002, with the necessary modifications;

(2) Seize any object of which he has reasonable grounds to believe that is an object connected with such an offense;

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

(b) For searching, seizing an object and accessing computer material or copying it under this Article, the provisions of Articles 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 a police officer shall be given to an investigator and the powers given to an officer shall be given to the Head of the Authority or an investigator authorized by him for that matter; notice of authorization under this subsection shall be published in the 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 provided for in subsection (a), the investigator may detain the person in order to ascertain the person's identity and address or to interrogate him at his location; 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; a person summoned to the offices of the Authority shall appear at the time he was summoned;

(2) For a delay under subsection (1), the provisions of Articles 66, 67 and 72 to 74 of the Detention Law shall apply, with the necessary modifications, and with the following changes: The powers given to the police officer shall be given to an investigator and the powers given to an officer shall be given to the Head of the Authority or to an investigator authorized by him for that matter, and the offices of the Authority declared by the Head of the Authority by a notice in the official gazette shall be deemed as a police station for the purposes of the Detention 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 if the following are met:

(1) The provisions under Article 23JA regarding the identification of an inspector apply to him, with the necessary modifications;

(2) He wears an investigator's uniform, in the color and form as determined by the Head of the Authority for this purpose, provided that such uniform does not appear to be a police uniform.

(b) The provisions of Article 23JB(b) and (c) shall apply, with the necessary modifications to the obligations under subsection (a).

Subchapter B: Offenses

23NC. Obstructing the Head of The Authority, Investigator or Inspector in the Performance of Duties

Obstructing the Head of the Authority, investigator or inspector in the performance of duties under this Law is subject to six months imprisonment.

23ND. Misleading the Head of The Authority, an Inspector or an External Expert

Conducting any of the following with the intention of misleading the Head of the Authority, an inspector, or an external expert, is subject to two years imprisonment:

(1) Providing incorrect details in an application for registration of a database submitted under Article 9 or in a notice of change in the details listed in Article 9(b) or in a notice under Article 8A(b);

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

23NE. Processing Data from a Database Without Authorization

Processing personal data from a database without authorization from the database controller, contrary to the provisions of Article 8(c), is subject to three years imprisonment.

23NF. Providing Incorrect Information When Requesting Data

Requesting from a person to receive personal data for its processing in a database while providing him with incorrect details, contrary to Article 11, with the intention of misleading him regarding the provision of the personal data, is subject to three years imprisonment.

23NG. Unlawful Data Transfer from a Public Body

A public body as defined in Article 23 that is a corporation, an employee of such a public body or who acts on behalf of such a public body, who provides personal data the transfer of which is prohibited under Article 23B, in order for an unauthorized party to process the data, is subject to three years imprisonment.

CHAPTER D5: Provisions Regarding Election

23NH. Definitions

In this chapter –

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

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

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

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

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

"The Local Authorities Law (Elections)" – The Local Authorities Law (Elections), 5725 -1965;

"Chairman of the District Election Committee" - the chairman of a regional election committee determined under Article 17D of the Elections Law (Propaganda Methods), regarding an election for a local Authority within the jurisdiction of the district court in which he serves;

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

(1) From the beginning of the period of the general election for local authorities 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 Article 25 of the Local Authorities Law (Elections);

(c) A person who is entitled, under Article 16(b)(1) of the Local Authorities Law (Elections), to receive data from the registry, and the information is provided to him under Article 16(c) of the said law;

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

(2) As of the date of submission of lists of candidates – a list of candidates in the election to the council of a local Authority and a candidate for the 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 election period for the Knesset that starts 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;

"Election periods" – the election period to the Knesset or the election period of general election to the local authorities;

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

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

"Authority election period" – 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 D1 and D3 During Election Periods

(a) The Head of the Authority, inspector or investigator shall not, during election periods, exercise his powers under the following Articles due to a violation of any of the provisions under this Law, relating to a database in which a party or a candidate in an election for a local Authority is the database controller, which they or a processor on their behalf carried out, unless he has received approval under subsection (b):

(1) Entering a place under Article 23J(a)(4);

(2) Submitting an application for a search and seizure order or an order for access to computer material within an administrative inquiry, pursuant to Article 23JD;

(3) Filing an application for a ban on processing order under Article 23MI;

(4) Power to seize any object, pursuant to Article 23NA(a)(2);

(5) Submitting an application for a search and seizure order or an order for access to computer material, pursuant to Article 23NA(a)(3);

(6) Notice of intent to charge under Article 23KG;

(7) The provision of an administrative notice, under Article 23LF;

(8) Providing a notice of the possibility of submitting a letter of undertaking and making a deposit, under Article 23LI.

(b) Powers under subsection (a) may be exercised—

(1) During the election period for the Knesset, regarding a database of which a party is the database controller – with the approval of the Chairman of the Central Election Committee;

(2) During the general 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 is the controller – with the approval of the chairman of the Central Elections Committee, and with regard to a database in which another candidate in the local authorities election is the controller – with the approval of the chairman of the Regional Elections Committee.

(c) Before granting approval under this Article, the chairman of the Central Elections Committee or the chairman of the Regional Election Committee, as applicable, shall give an opportunity to the party or candidate in the election of the local Authority concerned to argue their claims; however, with respect to the power under subsections (a)(1) to (5), the chairman of such an election committee may grant approval for the exercise of the Authority's power without asking for the position of the party or the candidate in the local Authorities elections, for reasons of urgency or if this would thwart the purpose of exercising the requested Authority's power; the circumstances of the case and the reasons for urgency will be included in the chairman's decision.

(d) The chairman of the Central Elections Committee or the chairman of a Regional Election Committee shall not give approval for the exercise of the Authority's powers under this Article, if he finds that doing so will materially impair the ability of the party or the candidate in the local Authorities elections, as applicable, to run in the elections or to manage the contact with the electorate, and that the severity of such expected harm exceeds the risk to infringement of privacy and the risk of harm to the public interest underlying the exercise of the Authority's power; such approval may be conditional.

(e) The chairman of the Central Elections Committee and the chairman of the Regional Elections Committee hearing a particular application may, on their own initiative, or upon a request of a party involved in the 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 under the circumstances.

(f) If the Head of the Authority, an inspector or an investigator decide to exercise powers under this Article during an election period for a local authority 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 the local authority is the controller, the candidate in the elections for the local authorities may request 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 – request the chairman of the Central Elections Committee, to determine that the requested power shall not be exercised during the election period for that local authority, if the provisions of subsection (d) apply, or to determine conditions for the exercise of such powers; the provisions of subsections (c) and (e) shall apply to such request and decision, with the necessary modifications.

(g) Proceedings under this Article will be subject to the provisions of Articles 17D and 17E of the Elections Law (Propaganda Methods), with the necessary modifications.

(h) The provisions of this Article shall apply, with the necessary modifications, to elections for other local authorities or to other regional councils that receive budget from the state budget, except for local committees.

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 infringed dies within six months after the infringement without having filed an action or complaint in respect thereof, his spouse, child or parent or, if he leaves no spouse, child or parent, his brother or sister may file an action or complaint in respect of that infringement within six months after his death.

(b) Where a person who has filed an action or complaint in respect of an infringement of privacy dies before the termination of the proceeding, his spouse, child or parent or, if he leaves no spouse, child or parent, his brother or sister may, within six months after his death, notify the court that he or she wishes to proceed with the action or complaint, and upon so notifying, he or she shall take the place of the plaintiff or complainant.

26. (Revoked)

27. Applicability of certain provisions of the Prohibition of Defamation Law

The provisions of Articles 21, 23 and 24 of the Prohibition of Defamation Law, 5725-1965, shall apply with the necessary modifications, as applicable, to legal proceedings for infringement of privacy.

28. Evidence as to a Person’s Bad Reputation, Character, or Past

In a criminal or civil proceeding for infringement of privacy, no evidence shall be produced, and no witness shall be examined, as to the bad reputation or as to the character, past, activities or opinions of the injured party.

29. Additional Orders

(a) In addition to any penalty and other relief, the court may, in a criminal or civil proceeding for infringement due to a violation of a provision of this law, order –

(1) The prohibition of the distribution of copies, or the confiscation of the infringing matter; a confiscation order under this subsection is effective against any person who has such material in his possession for sale, distribution or storage, also if he is not a party to the proceeding; where the court orders confiscation, it shall direct how the confiscated copies shall be disposed of;

(2) The publication of the whole or part of the judgment; the publication shall be made at the expense of the accused or defendant, in the place and in the dimensions and manner prescribed by the court.

(3) The surrender of the infringing matter to the injured party;

(4) The destruction of data unlawfully received, or the prohibition of use of the aforesaid data or of excess data as defined in section 23E, or any other order in respect of the data.

(b) The provisions of this section shall not prevent the keeping of a copy of a publication in public libraries, archives and the like unless the court, by a confiscation order under subsection (a)(1), imposes a restriction also on such keeping, and they shall not prevent the keeping of a copy of a publication by an individual.

29A. Statutory damages

(a) The court may order a person who has been convicted under Article 5 to pay the injured person statutory damages, that will not exceed 50,000 new shekels; an order for damages under this subsection shall be regarded as a ruling of the same court in a civil proceeding of the entitled against the person obliged.

(b) (1) In a civil proceeding under Article 4, the court may order that the defendant pay the plaintiff statutory damages that will not exceed 50,000 new shekels.

(2) In a proceeding under subsection (1) in which it was proven that the infringement of privacy was made with intent to cause harm, the court may order that the defendant pay the plaintiff statutory damages that will not exceed double the amount in that subsection.

(c) A person shall not be awarded statutory damages under this section, for the same infringement of privacy, more than once.

(d) The amounts in this section shall be updated on the 16th of each month, in accordance with the rate of change in the new index compared with the base index; in this regard-

"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. Responsibility for publication in newspaper

(a) Where an infringement of privacy is published in a newspaper, within the meaning of the Press Ordinance (hereinafter referred to as "a newspaper"), criminal and civil responsibility for the infringement shall be borne by the person who brought the material to the newspaper and thereby caused its publication, the editor of the newspaper and the person who actually decided upon the publication of the infringement in the newspaper, and civil responsibility shall be borne also by the publisher of the newspaper.

(b) In a criminal case under this Article, it shall be a good defense for the editor of the newspaper that he took reasonable steps to prevent the publication of the infringement or that he did not know of the publication.

(c) In this Article, "editor" of a newspaper includes the acting editor.

31. Liability of Printer and Distributor

Where an infringement of privacy is published in print, except in a newspaper published at intervals of not less than forty days, criminal and civil responsibility for the infringement shall be borne also by the possessor of the printing press, within the meaning of the Press Ordinance, in which the infringement was printed and by a person who sells or otherwise distributes the publication, provided that they shall not bear responsibility unless they knew or ought to have known that the publication contained an infringement of privacy.

31A. (Revoked)

31B. Civil Wrong

An act or omission in violation of the provisions of chapters B or D, or in violation of Regulations enacted under this Law, shall be a civil wrong under the Torts Ordinance [New Version].

32. Material Inadmissible as Evidence

Material obtained through infringement of privacy shall not be used as evidence in court without the consent of the injured party, unless the court, for reasons that shall be recorded, permits it to be used or if the infringer, being a party to the proceeding, has a defense or enjoys exemption under this Law.

33. Amendment of the Torts Ordinance

Article 34A of the Torts Ordinance [New Version] is hereby repealed.

34. Amendment of the Criminal Procedure Law

In the Schedule to the Criminal Procedure Law, 5725– 1965, the following subsection shall be added after subsection (12): "(13) offenses under the Privacy Protection Law, 57411981."

35. Preservation of Laws

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

36. Implementation of Regulations

The Minister of Justice is in charge of the implementation of this Law and may, with the approval of the Constitution Committee, make regulations as to any matter relating to its implementation, and *inter alia*:

(1) Conditions for retaining and storing of data in databases;

(2) Conditions for the transfer of data to, or from, databases abroad;

(3) Rules of conduct and ethics for database controllers or processors and their employees;

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

36A. Fees

(a) The Minister of Justice, with the approval of the Constitution Committee, may establish fees for accessing a database 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. 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 Article 3)

Government Resolution No. 1890

Resolution:
Further to Government Resolution No. 4660 dated 19 January 2006, Government Resolution No. 4820 dated 28 June 2012, and Government Resolution No. 3019 dated 7 September 2017, as follows:

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 performing its duties, through the Authority's employees, and in accordance with the provisions of any law, and the Authority's operational budget shall be managed separately within the Ministry of Justice's budget. Respecting the Authority's independence, the Authority shall act autonomously when exercising the powers vested in the Head of the Authority.
2. The Authority's duties are, *inter alia*, as follows:
   (a) Monitor compliance with the provisions of the Privacy Protection Law, 5741-1981 and the Regulations promulgated thereunder with regard to databases.
   (b) Investigate suspicions of an offense being committed under the Privacy Protection Law, 5741-1981 with regard to databases, in accordance with its powers under law.
   (c) 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 public campaign.
   (d) Handle public inquiries where there are grounds for harming data subjects under the Privacy Protection Law, 5741-1981.
   (e) Develop and implement professional programs and training in its fields of activity.
   (f) Promote and maintain contacts with corresponding entities worldwide and within international forums in which corresponding entities take part.

(g) Exercise the powers of the Registrar of Certification Authorities under the Electronic Signature Law, 5761-2001.

3.

(a) Further to Government Resolution No. 4660 dated 19 January 2006 and Government Resolution No. 3543 dated 11 February 2018, determine that the job qualifications for appointment as Head of the Authority will be as follows:

(1) A person qualified to be appointed as a District Court Judge.

(2) No person who has been convicted of a criminal offense or a disciplinary offense which due to its essence, severity or circumstances, is not fit for serving as Head of the Authority, or has been indicted or served with a private complaint for such an offense, and a final court ruling regarding him has yet to be given, will be appointed as Head of the Authority.

(b) It should be clarified that in accordance with Government Resolution No. 4470 dated 8 February 2009, the Head of the Authority shall be appointed for one six-year term.

4. Amend Government Resolution No. 4660 dated 19 January 2006, and determine that:

(a) The Government shall appoint the Head of the Authority, by publication in the official gazette, as Registrar according to Article 7 of the Privacy Protection Law, 5741-1981

(b) The Minister of Justice shall appoint the Head of the Authority as Registrar according to Article 9 of the Electronic Signature Law, 5761-2001.

Schedule 2

(Subsection (12) of the definition "data of special sensitivity", in Article 3)

(1) Data about membership in a trade union as defined in Article 7 of the Privacy Protection Regulations (Instructions regarding data transferred to Israel from the European Economic Area), 5783-2023.

Schedule 3

(Article 23KF(h))

Monetary Sanction for Violating the Data Security Regulations

In this Schedule –

"external service provider" – as defined in Article 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, offspring of a spouse, 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" – database of which the controller is an individual, or a corporation owned by an individual or a cooperation owned by two individuals, in which only the individual and at most two more are authorized users for its use, and are able to use the database, not including the following databases:

(1) A database whose main purpose is to collect personal data for providing it 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 which contains personal data in respect of which the database controller 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 main purpose is not to collect personal data for the providing it to another as a business practice or for consideration, including direct mailing services;

(2) The database controller is not a public body as defined in Article 23;

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

(a) The number of authorized users to the database 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, that is used for the sole purpose of the database controller's business management, and is only of one of the following types:

(1) Data under subsections (2), (6), and (8) to (10) of the definition of "data of special sensitivity";

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

(3) Personal data about their religious beliefs;

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

"database subject to the medium 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 main purpose is to collect personal data for providing it to another as a business practice or for consideration, including direct mailing services;

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

(3) The database includes data of special sensitivity, except for data of special sensitivity excluded in subsection (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 defined in section (1) of the definition of a "database subject to the medium security level" or a database containing data of special sensitivity and the number of authorized users 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" – Privacy Protection Regulations (Data Security) 5777-2017.

Violation	Monetary sanction amount (in NIS)			
Column A	Column B – database managed by an individual	Column C – database subject to the basic security level	Column D –database subject to the medium security level	Column E – database subject to the 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 Article 2(a) of the Data Security Regulations, contrary to the provisions of that Article, including the different types of data held in the database pursuant to subsection (3), taking into account the list of types of data that constitute data of special sensitivity under Article 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, contrary to Article 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 reviewed or documented the review of whether the data it holds in the database exceeds what is required for the purposes of the database, contrary to Article 2(c) or 19(b) of the Data Security Regulations.	2,000	2,000	40,000	160,000
(4) Preparation of a data security procedure: A database controller or processor that has not prescribed a written data security procedure in accordance with the database definitions document and the Data Security Regulations (hereinafter – security procedure), contrary to the provisions of Article 4(a) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	2,000	40,000	160,000

(5) Security procedure – preparation, securement, and instruction setting: A database controller or processor that has not done one of the following: (a) Secured the security procedure so that details from it are provided to authorized users only to the extent necessary for the performance of their duties, contrary to Article 4(b) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable; (b) Included in the security procedure the details listed in Article 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 Article 4(d) of the Data Security Regulations or to the provisions listed in Article 9(b)(2) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable; (c) prescribed in the security procedure instructions regarding the handling of data security incidents or regarding reporting to the database controller, contrary to Article 11(b) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable; (d) Included in the security procedure the matters listed in Article 15(a)(2)(a) to (e) of the Data Security Regulations, contrary to the provisions of Article 15(a)(3) of the Regulations.	–	2,000	40,000	160,000
(6) Database structure and systems: A database controller or processor that has not maintained an up-to-date document of the database's structure or an up-to-date inventory list of the database's systems, under Article 5(a) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	1,000	20,000	80,000

(7) Provision of details on the database's structure and inventory list: A database controller or processor who has not kept the up-to-date database structure document or the inventory list in accordance to the access authorizations determined under Article 5(b) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	1,000	20,000	80,000
(8) Protection of systems: A database controller or processor that has not ensured that the systems specified in Article 5(a)(1) of the Data Security Regulations are maintained in a secure place that prevents unauthorized penetration and entry, which is suitable to the nature of the database's activity and the sensitivity of the data therein, in accordance with Article 6(a) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	1,000	1,000	20,000	80,000
(9) Risk assessment: A database controller or processor 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 conducted a discussion on the findings of the risk assessment that were provided and has not examined the need to update the database definitions document or the security procedure as a result, or has not acted to rectify deficiencies found in the course of the risk assessment, contrary to Article 5(c) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	–	–	320,000
(10) Penetration tests: A database controller or processor that has not ensured that penetration tests are conducted on the database's systems at least once every 18 months, or has not conducted a discussion on the results of the penetration tests or has not acted to rectify deficiencies identified, contrary to Article 5(d) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	–	–	320,000

(11) Monitoring and documentation of site access: a database controller or processor that has not taken measures to monitor and document in accordance with Article 6(b) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	–	20,000	80,000
(12) Manpower management: a database controller or processor that has granted access to data held in the database or changed the scope of the authorization granted, without taking any reasonable measures under Article 7(a) of the Data Security Regulations, contrary to the provisions of that Article or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	1,000	20,000	80,000
(13) Manpower training: A database controller or processor that has granted access to data held in the database or changed the scope of the authorization granted, without first providing training or providing the required information to the authorized users, contrary to the provisions of Article 7(b) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	1,000	20,000	80,000
(14) Periodic training: A database controller or processor that has not conducted periodic training for its authorized users, contrary to Article 7(c) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	–	20,000	80,000
(15) Determining and management of access permissions: a database controller or processor that has not determined access permissions for authorized users to the database and the database's systems, contrary to Article 8(a) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable, or has not kept an up-to-date record of valid permissions, contrary to the provisions of Article 8(b) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable (hereinafter - list of valid permissions).	–	2,000	40,000	160,000

(16) Implementation of access permission procedure: A database controller or processor that has not taken appropriate measures under the circumstances and according to the nature and kind of database, in order to ensure that access to the database and database's systems is made only by authorized users according to the list of valid permissions, contrary to Article 9(a) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	2,000	2,000	40,000	160,000
(17) Implementation of access permission procedure with respect to an authorized user who has finished his role: a database controller or processor that has not ensured the revoking of authorizations granted to an authorized person who no longer in his role, contrary to Article 9(c) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	2,000	40,000	160,000
(18) Access monitoring and documentation mechanism: A database controller or processor that has not done one of the following: (a) Ensured that a monitoring mechanism is in place, contrary to Article 10(a) and (b) of the Data Security Regulations (hereinafter – monitoring mechanism) or its provisions as applied in Article 19(a) of the Regulations, as applicable; (b) Prescribed a routine procedure to examine the records of the monitoring mechanism and prepared a report of the issues found and the measures taken as a result, contrary to Article 10(c of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable; (c) Ensured that the records of the monitoring mechanism are retained for at least 12 months, contrary to Article 10(d) of the Data Security Regulations or its	–	–	40,000	160,000

provisions as applied in Article 19(a) of the Regulations, as applicable; Informed the authorized database users of the existence of the monitoring mechanism, contrary to Article 10(e) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.				
(19) Data security incident documentation: a database controller or processor that has not ensured the documentation of any event in which an incident was discovered that raises concern regarding a breach of data integrity, unauthorized use, or deviation from authorization (hereinafter – data security incidents), contrary to Article 11(a) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	2,000	2,000	40,000	160,000
(20) Periodic discussion on data security incidents: A database controller or processor that has not held a discussion regarding data security incidents or has not assessed the need to update the security procedure and documented such discussion and assessment, contrary to Article 11(c) and Article 19(b) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	–	40,000	160,000
(21) Reporting to the Privacy Protection Authority regarding a severe security incident: A database controller or processor that has not immediately notified the Head of the Authority of a severe security incident, or has not reported to the Head of the Authority about the measures taken following the incident, contrary to Article 11(d)(1) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	–	80,000	320,000
(22) Updating the database's systems: a database controller or processor that has not ensured that updates to the database's systems are conducted on a regular basis, including the computer material required for their operation, or that no use is made of systems where the security aspects are not supported by the manufacturer without a security solution, contrary to Article 13(c) of the Data Security Regulations or its provisions as	2,000	2,000	40,000	160,000

applied in Article 19(a) of the Regulations, as applicable.				
(23) Network security: a database controller or processor that has connected the database's systems to the internet or to another public network without installing any safeguard, contrary to Article 14(a) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	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 service provider to receive services, and has not explicitly determined in the agreement with that provider the matters listed in Article 15(a)(2) of the Data Security Regulations or has not taken any monitoring and supervision measures over the external service provider's compliance with the provisions set forth in the agreement regarding the matters detailed in subsections (d) and (f) to (h) in that Article, contrary to the Article 15(a)(4) of the Data Security Regulations.	–	4,000	80,000	320,000
(25) Documentation: a database controller or processor that has not retained in a secure manner, for at least one year, the data collected when implementing Articles 6(b), 8-11, 14, 15(a)(4) and 16 of the Data Security Regulations, that apply to it, contrary to Article 17(a) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	1,000	20,000	80,000
26) Backup of documentation data: a database controller or processor that has not done one of the following: (a) Backed up retained data in a manner ensuring that the data can be restored to its original form at all times, contrary to Article 17(b) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable; (b) Prescribed in a document the matters listed in Article 18(a)(1) and (3) of the Data Security Regulations and has also established procedures to ensure data	–	–	20,000	80,000

restoring, under Article 17(b) to the Regulations; (c) Ensured that a backup copy of the data and the procedures provided for in Article 18(a) of the Data Security Regulations are retained in a manner that ensures the integrity of the data and the ability of restoring the data, contrary to Article 18(b) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.				
(27) Violation of documentation obligation: A database controller or processor that has not documented the manner in which it performed an action it is obligated or responsible to perform under the Regulations, and that action is not the creation of a document, contrary to Article 19(b) of the aforementioned Regulations.	–	1,000	20,000	80,000
(28) Separation of the database's systems (compartmentalization): a database controller or processor that has not separated between the database's systems that enable access to personal data, and other computer systems used by it, contrary to Article 13(b) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	–	20,000	80,000
(29) Periodical audit: a database controller or processor that has not ensured that an internal or external audit is conducted at least once every 24 months, contrary to Article 16(a) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable or has not conducted a discussion on the audit reports that were provided to it, or has not assessed the need to update the database definitions document or the security procedure accordingly, contrary to Article 16(c) of the Data Security Regulations or its provisions as applied in Article 19(a) of the Regulations, as applicable.	–	–	40,000	160,000

Schedule 4

(Article 23KF(i))

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

In this Schedule, "Regulations on the Transfer of Data from the European Economic Area" – the Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5789-2023.

Part A

<table>
<tr><th>Column A
The Violation</th><th>Column B
Monetary sanction
Amount</th></tr>
<tr><td>(1) A database controller that has not notified the data subject, in writing, of its decision in the application under Article 3(a) of the Regulations on the Transfer of Data from the European Economic Area, contrary to Article 3(d) of the Regulations.</td><td>15,000</td></tr>
<tr><td>(2) A database controller that has not implemented any organizational, technological, or other mechanism, the purpose of which is to ensure that the database does not include data that are no longer necessary for the purpose for which it was collected or retained or for any other purpose for which it may be retained in accordance with any law (hereinafter – unnecessary data), contrary to Article 4(a) of the Regulations on the Transfer of Data from the European Economic Area.</td><td rowspan="3">An amount of 2 new shekels for each person about whom personal data are held in the database, and if the personal data in the database are 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 data are 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 processor in the amount of 20,000 new shekels or 40,000 new shekels, as applicable.</td></tr>
<tr><td>(3) A database controller that has not implemented any organizational, technological, or other mechanism, the purpose of which is to ensure that the data in the database are correct, complete, clear, and updated, contrary to Article 5(a) of the Regulations on the transfer of information from the European Economic Area.</td></tr>
<tr><td>(4) A database controller that has found that the database contains data that are not correct, complete, clear, or updated, and that has not taken any measures to rectify or delete the data, contrary to Article 5(b) of the Regulations on the transfer of information from the European Economic Area.</td></tr>
</table>

Part B

<table>
<tr><td>(1) A database controller that received a written request for the deletion of personal data under Article 3(a) of the Regulations on the Transfer of Data from the European Economic Area, and the exclusions under Article 3(b) of the Regulations do not apply, and did not delete the data or took actions to ensure that it will be impossible, by applying reasonable measures, to identify the data subject, contrary to Article 3(c) of the Regulations, and after receiving a notice from the Head of the Authority under Article 23KE(c), according to which its actions constitute a violation, did not cease the violation within the time period instructed by him.</td><td rowspan="4">An amount of 4 new shekels for each person about whom personal data are held in the database, and if the personal data in the database are data of special sensitivity – an amount of 8 new shekels for each person; If the amount of the monetary sanction is less than 200,000 new shekels, the Head of the Authority may impose on the database controller or processor 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 individuals about whom the database controller did not delete personal data as required or did not provide them with a notice as required under Articles 3(c) or 6(a) or 6(b) of the Regulations on the Transfer of Data from the European Economic Area, as applicable.</td></tr>
<tr><td>(2) A database controller that has found that the database contains personal data that is unnecessary according to Article 4(b) of the Regulations on the transfer of data from the European Economic Area and has not taken actions that ensure that it will be impossible to identify the data subject as set forth in Article 4(c), and the circumstances set forth in that Article did not apply, and has not deleted the aforementioned data at the earliest opportunity under the circumstances, contrary to Article 4(b) to the Regulations, and after receiving a notice from the Head of the Authority under Article 23KE(c) according to which its actions constitute a violation, did not cease the violation within the time period instructed by him.</td></tr>
<tr><td>(3) A database controller that received personal data about a person and did not notify him as required under Article 6(a) of the Regulations on the Transfer of Data from the European Economic Area, and none of the circumstances set forth in Article 6(c) of the Regulations apply, contrary to Article 6(a), and after receiving a notice from the Head of the Authority under Article 23KE(c) according to which its actions constitute a violation, did not cease the violation within the time period instructed by him.</td></tr>
<tr><td>(4) A database controller who intended to transfer the personal data it received to a third party and did not provide notice to the data subject as required under Article 6(b) of the Regulations on the Transfer of Data from the European Economic Area, and none of the circumstances set forth in Article 6(c) of the Regulations apply, contrary to Article 6(b), and after receiving a notice from the Head of the Authority under Article 23KE(c) according to which its actions constitute a violation, did not cease the violation within the time period instructed by him.</td></tr>
</table>

Schedule 5

(Section 23LA)

Reduced Amounts Regarding a Monetary Sanction

1. Definitions

In this Schedule –

"Certificate Regarding Turnover" – 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 association – a certificate issued by a person who audited the accounts of the cooperative association under Article 20 of the Cooperative Associations Ordinance;

(3) Regarding any other violator – a certificate issued by a certified public accountant or a tax advisor representing the violator, confirming that the turnover amount presented by the violator corresponds with the amount stated in a document submitted to the Israel Tax Authority or to the National Insurance Institute under the law; for this purpose, "tax advisor representing" – as defined in the Representative work by Tax advisors 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 the second Schedule of 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 violation 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 violation 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 violation of the provision for which a monetary sanction is imposed on the violator, no monetary sanction or administrative enforcement measure under Chapters B to E of Chapter D'3 was imposed on it for a violation of the same provision – by 20%; if no monetary sanction or administrative enforcement measure as aforesaid was imposed on the violator in the three years preceding the violation – by 10%;

(2) The violator ceased the violation on its 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 data protection officer only under Articles 17B1(a)(3) and (4), and appointed such an officer before the notice of intent to charge was delivered – by 10%; this reduction shall apply as long as the Minister of Justice has not, with the approval of the Constitution Committee, made an order under Article 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 that was paid or ordered to be paid by 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 as a result of personal circumstances justifying a reduction of the monetary sanction or that severe personal circumstances exist that justify leniency 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 under Articles 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 it by the percentages provided for these 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-enterprise or small enterprise, as applicable, he shall reduce the amount of the monetary sanction imposed on it, whether or not they were reduced under Article 2, 3 or 4, so that the amount of the sanction for violations under each of the subsections listed below shall not exceed the amount specified for them:

(1) Regarding violations listed in Article 23KF(a) and (b), in subsections (6) to (8), (11) to (14) and (25) to (28) of the third Schedule, and subsection (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 Article 23KF(c) to (f), in subsections (1) to (5), (9) and (10), (15) to (24) and (29) of the third Schedule, in subsections (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 Article 23KF(g) – for a micro-enterprise – 70,000 new shekels, and for a small enterprise – 140,000 new shekels

If a violator that is a micro-enterprise or a small enterprise violates several provisions under subsections (1) to (3), the violator shall not be liable for 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 Article 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 dealer with no turnover, the Head of the Authority shall not reduce the amount of the sanction under this Article to an amount less than the maximum amount that may be imposed under Article 6 regarding a micro-enterprise.

(b) A violator requesting a reduction of the amount of the monetary sanction under Article 6 or under this Article shall submit to the Head of the Authority a certificate regarding turnover within 30 days from the date of delivery of the notice of intent to charge.