Privacy Protection Regulations (Instructions for Data that was Transferred to Israel from the European Economic Area), 5783-2023

Pursuant to my authority under sub-Article (2) of the definition of "sensitive data" in Article 7 and under Article 36 of the Privacy Protection Law 5741-1981 (hereinafter – "the Law"), and with the approval of the Knesset Constitution, Law and Justice Committee, I hereby enact the following Regulations:

Definitions

1. In these regulations –
"European Economic Area" – EU Member States as well as Iceland, the Kingdom of Norway and the Principality of Liechtenstein;
"Data subject" – as defined in the Data Security Regulations;
"Data Security Regulations" – the Privacy Protection Regulations (Data Security) 5777-2017.

Application

2. (a) These regulations will apply to:

(1) Data that is in a database in Israel that has been transferred from the European Economic Area, except for data that a natural person directly provided on his initiative.
(2) Any other data that is in a database in Israel that contains data as stated in sub-regulation (1).

(b) Notwithstanding the provisions of sub-regulation (a), the obligations stated in these regulations will not apply to:
(1) Data transferred from an authority in the EEA responsible for national security or criminal law enforcement to a Security Agency as defined in Article 19 (c) of the Law.
(2) The use of data, required for the protection of national security or criminal law enforcement, to the extent necessary and proportionate for these purposes.

Data deletion

3. (a) A database controller will delete data, after receiving the written request of the data subject, if one of the following applies:

(1) The data was created, obtained, accrued or collected in contravention of the provisions of any law, or that the further use of the data is in violation of the law;

(2) The data is no longer necessary for the purposes for which it was created, obtained, accrued or collected;

(b) Notwithstanding the provisions of sub-regulation (a), a database controller may refuse a request to delete data, to the extent the use of the data is necessary and proportionate for one of the following:

(1) Exercising the right of freedom of expression, including the public's right to know.

(2) Performing a legal obligation or exercising an authority by operation of the law;

(3) Protecting a public interest, including for archival purposes, scientific research or statistical research;

(4) Conducting a legal proceeding or ensuring debt collection;

(5) Addressing fraud, theft or other incidents affecting the integrity of the data processing operations;

(6) Fulfilling an obligation resulting from an international agreement to which the Government of Israel is a party.

(c) If an application was received in the manner prescribed under sub-regulation (a), and the database controller found that the exclusions set out in sub-regulation (b) do not hold true, the database controller will delete the data under his control, or conduct actions that will assure that it is impossible, by applying reasonable measures, to identify the data subject.

(d) The database controller will notify, in writing, the data subject regarding his decision in the application at the earliest opportunity in the circumstances of the case.

Data retention

4. (a) The database controller will have in place an organizational, technological or other mechanism, the purpose of which is to ensure that the database does not include data that is 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 – "Data that is not necessary".

(b) If the database controller finds, on the basis of, *inter alia*, the mechanism set out in sub-regulation (a), that data that is not necessary is kept in the database, he shall delete the said data at the earliest opportunity in the circumstances of the case.

(c) The duty prescribed under sub-regulation (b) shall not apply if actions that assure that it is impossible, by applying reasonable measures, to identify the data subject, were performed with respect to the said data, or to the extent the use of the data is necessary and proportionate for one of the following:

(1) Exercising the right of freedom of expression including the public's right to know;

(2) Protecting a public interest, including for archival purposes, scientific research or statistical research;

(3) Conducting a legal proceeding or ensuring debt collection;

(4) Addressing fraud, theft or other incidents affecting the integrity of the data processing operations;

(5) Fulfilling an obligation resulting from an international agreement to which the Government of Israel is a party.

Data accuracy

5. (a) The database controller will have in place an organizational, technological or other mechanism, the purpose of which is to ensure that the data in the database is correct, complete, clear and updated.

(b) If the database controller finds, on the basis of, *inter alia*, the mechanism set out in sub-regulation (a), that the database contains data that is not correct, complete, clear or updated, he will take reasonable measures in the circumstances of the case for the purpose of rectifying or deleting the data.

Duty to inform

6. (a) A database controller who received data about a person will inform the said person, whether directly or indirectly, by the entity that provided the data from the European Economic Area, and as shortly as possible after receiving the data and no later than one month as of the date of receiving the data, regarding all of the following:

(1) The identity of the database controller and the database manager, their addresses and contact information;

(2) The purpose of the transfer of the data;

(3) The type of the data that was transferred;

(4) The existence of the right to deletion, pursuant to Regulation 2, a right to access the data, pursuant to Article 13 of the Law, and the right to correct data, pursuant to Article 14 of the Law.

(b) If a database controller requests to transfer data he received to a third party, the database controller will notify the data subject, whether directly or indirectly, by the entity from which the data was transferred from the European Economic Area, at the earliest opportunity, and no later than the time of the data transfer, about each of the following:

(1) The identity and the contact information of the third party or the categories of third party recipients to whom the data will be transferred;

(2) The purpose of transfer of the data;

(3) The type of the data that will be transferred;

(4) The existence of the right to deletion, pursuant to Regulation 3, a right to access the data, pursuant to Article 13 of the Law, and the right to correct data, pursuant to Article 14 of the Law.

(c) The duty to inform as stated in sub-regulations (a) or (b) will not apply if one of the following holds true, and this is to the extent necessary and proportionate in the circumstances of the case:

(1) The database controller has reasonable grounds to assume that the particulars of the data that are included under sub-regulations (a) or (b) are known to the data subject;

(2) The contact information of the data subject is not known to the database controller, or the implementation of the duty to inform involves an unreasonable burden on the database controller, taking also into account the possibility to cooperate with the data exporter;

(3) The existence of a duty of confidentiality prescribed by law or a prohibition by law on the disclosure of the data;

(4) The existence of a legal provision that regulates the disclosure of the particulars of the data as stated in sub-regulations (a) or (b);

(5) Exercising the duty to inform may harm a person's life, health or body;

(6) Exercising the duty to inform may harm journalistic activities or reveal the source of information for journalistic activity;

(7) Exercising the duty to inform will affect the rights of a person in a degree exceeding the harm caused to the data subject as a result of failure to disclose the particulars of the data pursuant to regulations (a) or (b);

Sensitive Data

7. Data that has been transferred to a database in Israel as stated in regulation 2 on the subjects specified below, shall be considered sensitive data under Article 7 of the Law:

(1) Data regarding a person's ethnic origin;
(2) Data regarding trade union membership.

Reservation of Law

8. Nothing in these regulations –
Shall prejudice other obligations imposed on a database controller by law.
Shall permit use of data that is not permitted in accordance with any law.

Commencement and application

9. These Regulations will commence-

(1) Regarding data as stated in sub-regulation 2(a)(1)

(a) Three months as of the date of their publication (hereinafter – the "determining day") regarding data received in a database in Israel on or after the determining day;

(b) One year from the date of their publication - regarding data received in a database in Israel before the determining day.

(2) Regarding data as stated in sub-regulation 2(a)(2) – 1.4.5785 (January 1st 2025).