PROTECTION OF PRIVACY REGULATIONS (DATA SECURITY) 5777-2017*

By the power vested in me pursuant to Article 36 of the Protection of Privacy Law 5741-1981 (the "Law") and with the approval of the Knesset Constitution, Law and Justice Committee, I hereby promulgate these Regulations:

Definitions

1. In these Regulations –

"Severe security incident" - any of the following:

(1) In a database subject to high security level - an incident involving the use of data from the database without authorization or in excess of authorization, or damage to the data integrity;

(2) In a database subject to medium security level - an incident involving the use of substantial part of the database without authorization or in excess of authorization, or damage to the data integrity with respect to a substantial part of the database;

"Authorized user" - a person who has access to one of the following with the permission of the database controller or processor:

(1) Data from the database;

(2) Database systems;

(3) Information or component which is required for operating or accessing the database;

Notwithstanding the above, a processor who is not an individual, or an individual who obtained access on the basis of the processor's permission, will not be considered an authorized user of the database controller;

"Portable device" - any of the following:

(1) A computer intended for mobile use, including a computer which is radio telephone end equipment as defined in the Wireless Telegraph Ordinance [New Version] 5732-1972;

(2) Other medium used to store computer material;

"Computer material" and "computer" - as defined in the Computers Law 5755-1995;

"Database managed by an individual" - a database managed by an

* Published Regulations File 5777 no. 7809 dated 8.5.2017 p. 1022.

individual or by a corporation owned by an individual, in which only the individual and at most two more authorized users are permitted to use, and are able to use the database, with the exception of the following databases:

(1) A database whose main purpose is collecting data for the purpose of transferring it to a third party as part of regular professional activity, including direct mailing services;

(2) A database which contains information about 10,000 or more persons;

(3) A database which contains information in respect of which the database controller is subject to a professional duty of confidentiality by law or professional ethical principles;

"Databases subject to basic security level" - databases that are not of the kinds enumerated in the First or Second Schedule, and are not a database managed by an individual;

"Databases subject to medium security level" - databases of the kinds enumerated in the First Schedule, and are not a database managed by an individual;

"Databases subject to high security level" - databases of the kinds enumerated in the Second Schedule, and are not a database managed by an individual;

"Biometric data" - information used to identify a person which is a unique physiological human characteristic that can be measured by a computer;

"Data security officer" - as defined in Section 17B of the Law;

"Database systems" - systems serving the database which are important for information security aspects;

"The data subject" - the person on which the database contains information;

"National Cyber Defense Authority" - the National Cyber Defense Authority designated to protect the cyberspace, as established pursuant to a Government Resolution and acting in accordance with its resolutions;

"A public network" - a communication network that allows its usage also by those who are not authorized users.

Database definitions document

2. (a) A database controller will specify in the database definitions document (the "database definitions document") at least the following matters:

(1) A general description of the data collection and usage activities;

(2) A description of the purposes for which the data is used;

(3) The types of data contained in the database, in accordance with the list of data types in Item 1(3) of the First Schedule;

(4) Details regarding the transfer of the database or substantial parts thereof outside the State borders or the use of the data outside the State borders, the purpose of transfer, country of destination, manner of transfer and the identity of the transferee;

(5) Data processing activities by a processor;

(6) The main risks concerning a breach of information security and the manner in which they are dealt with;

(7) The name of the database manager, the database processor and the data security officer, if appointed.

(b) The database controller will update the database definitions document whenever a significant change has been made to the matters detailed in Sub-Regulation (a) and will annually assess, by 31 December of each year, the need for such an update due to technological changes within the organization or security incidents as per Regulation 11.

(c) The database controller will review annually whether the data stored in the database exceeds what is required for the database purposes.

Data security officer

3. Where there is a duty to appoint a data security officer, or where a data security officer of the database has been appointed, the following provisions shall apply:

(1) A data security officer will directly report to the database manager or to an active manager of the database's controller or processor, as appropriate, or to another senior official who directly reports to the database manager;

(2) The data security officer will prepare a data security procedure and have it approved by the database controller;

(3) The data security officer will prepare a plan for regular monitoring in regard to compliance with these Regulations, implement this plan and notify the database controller and the database manager of his findings;

(4) The data security officer will not perform an additional role which may put him at risk of conflict of interest while performing his role according to these Regulations;

(5) Where a database controller assigns the data security officer tasks that are additional to the duties listed in Paragraphs (2) and (3) for the purpose of implementing these Regulations, they will be clearly defined;

(6) A database controller will allocate to the data security officer the necessary resources for carrying out his role.

Data security procedure

4. (a) A database controller will prescribe a written data security procedure ("the Procedure") according to the database definitions document and these Regulations. The Procedure will be binding upon each one of the authorized users depending on the parts of the Procedure that are disclosed to him in accordance with Sub-Regulation (b).

(b) A database controller will retain the Procedure in such a manner that details from the Procedure will be disclosed to authorized users only to the extent required for performing their role.

(c) The Procedure will include, inter alia, the following:

(1) Instructions concerning physical protection of the database sites and their surroundings as per Regulation 6;

(2) Access authorizations to the database as well as to database systems pursuant to Regulation 8;

(3) Description of the means intended to protect the database systems and the manner of their operation for this purpose;

(4) Instructions to authorized users of the database and database systems regarding the protection of data stored in the database;

(5) The risks to which the data in the database is exposed in the course of the database controller's ongoing activities, including those originating from the database systems structure as detailed in Regulation 5(a), the manner in which these risks are identified and dealt with, including by commonly used encryption mechanisms to protect the data stored in the database or in the database systems;

(6) The manner of dealing with information security incidents as per Regulation 11, according to the severity of the incident and information sensitivity level;

(7) Instructions concerning the management and usage of portable devices pursuant to Regulation 12.

(d) In a database subject to medium or high security level, the Procedure will address, in addition to the provisions of Sub-Regulation (c), also the following:

(1) Identification and verification measures with respect to access to the database and to the database systems, pursuant to Regulation 9;

(2) The manner of monitoring the use of the database, including the documentation of accessing the database systems pursuant to

Regulation 10;

(3) Instructions with respect to conducting periodical audits to ensure that appropriate security measures, in accordance with the Procedure and these Regulations as per Regulation 16, are in place;

(4) Instructions regarding backup of the data as noted in Regulation 18(a)(1);

(5) Instructions regarding the manner in which development activities in the database are performed and documented, including the manner developers may access the data in the database.

(e) The database controller will annually assess the need to update the Procedure and, irrespective of this, will assess whether the Procedure should be updated in the following instances:

(1) Material modifications in the database systems or data processing processes are carried out;

(2) New technological risks relating to the database systems have become known.

(f) An organization that controls several databases may prescribe a data security procedure according to this Regulation in a single document which concerns all databases it controls that have the same security level.

Mapping the database systems and performing a risk assessment

5. (a) A database controller will maintain an up-to-date document of the database structure, as well as an up-to-date inventory of the database systems, including:

(1) Infrastructure and hardware systems, types of communication and data security components;

(2) The software systems used to operate, administer and maintain the database, to support its activity, monitor it and secure it;

(3) Software and interfaces used for communication to and from the database systems;

(4) A diagram of the network in which the database is operating, including a description of the connections between the different system components and the physical location of these components;

(5) The date in which the document and the inventory were last updated.

(b) The up-to-date database structure document and inventory will be

secured in such a manner that only authorized users who require them for the performance of their role will be provided access.

(c) In a database subject to high security level, the database controller is responsible to conduct a data security risk assessment (the "risk assessment"); the database controller will discuss the findings of the risk assessment provided to him, consider the need to update the database definitions document or the data security procedure as a result, and act to amend the shortcomings found in the course of the assessment, if any; such risk assessment will take place at least once every eighteen months.

(d) In a database subject to high security level, the database controller is responsible to conduct, at least once every eighteen months, penetration tests to the database systems in order to test their vulnerability to external and internal threats; the database controller will discuss the results of the penetration tests and act to amend the faults found, if any.

(f) An organization that controls several databases may prescribe the inventory pursuant to Sub-Regulation (a) in a single document covering all databases it controls that have the same security level, and may also perform the duties prescribed in Sub-Regulations (c) and (d) in a single risk assessment or in a single penetration test, as relevant, with respect to all databases he owns that have the same security level.

Physical protection and secure surroundings

6. (a) A database controller will ensure that the systems listed in Regulation 5(a)(1) are maintained in a secure place, preventing unauthorized penetration and entry, and which is suitable to the nature of the database activity and the sensitivity of information therein.

(b) A controller of a database subject to medium or high security level will take measures to monitor and document the entry to and exit from sites in which the systems listed in Regulation 5(a)(1) are located, as well as the setting and removing of equipment in and from the database systems.

Data security in manpower management

7. (a) A database controller will not grant access to information stored in the database and will not change the scope of authorization granted, unless he took reasonable measures, commonly used in the processes for screening and placing employees, to ensure that there is no concern that the authorized user is not suitable to be granted access to information stored in the database; such measures will be taken in accordance with the sensitivity of the information in the database and the scope of access permissions attached to the role proposed to the relevant person, pursuant to Regulation 8.

(b) Before users gain access to the database or before a change in the scope of their authorizations, the database controller will hold training sessions for authorized users regarding the obligations embodied in the Law

and Regulations, and provide them information regarding their duties according to the Law and the data security procedure.

(c) In a database subject to medium or high security level, the database controller will hold periodical training to authorized users regarding the database definitions document, data security procedure and the data security provisions embodied in the Law and Regulations, as necessary for performing their role, and the duties that they impose on authorized users; such training shall take place at least once every two years, and with respect to certifying a new authorized user for a new role - as soon as possible after he was certified.

Access permissions management

8. (a) A database controller will determine access permissions of authorized users to the database and database systems in accordance with the role's responsibilities; access permission will be granted only to the extent required for performing the role.

(b) A database controller will keep an up-do-date record of roles, user permissions granted to these roles and the authorized users performing such roles (the "valid authorizations list").

Identification and authentication

9. (a) A database controller will take appropriate measures under the circumstances, and according to the nature and kind of the database, in order to ensure that only authorized users, according to the valid authorizations list, are using the database and the database systems.

(b) In a database subject to medium or high security level -

(1) The identification manner will be, as much as possible, by a physical mean subject to the exclusive control of the authorized user;

(2) The data security procedure will also prescribe instructions with respect to Sub-Regulation (a), including in the following matters:

(a) The manner of identification; in case the manner of identification is based on passwords, the Procedure will also address the password strength, number of failed attempts and the frequency of changing passwords that will take place according to the authorized user's role, and in any event, at least every six months;

(b) Automatic disconnection following a time of inactivity;

(c) The manner of dealing with malfunctions related to identity authentication.

(c) Immediately following the termination of an authorized user's role, a database controller will ensure revoking the permissions of an

authorized user who stopped working in his role, and as much as possible, changing the passwords to the database and database systems which the authorized user could have known.

Monitoring and documenting access

10. (a) In the systems of a database subject to medium or high security level, an automatic recording mechanism shall enable monitoring the access to the database systems (in this Regulation - "monitoring mechanism"), including the following data: user identity, date and time of access attempt, system component to which access was attempted, access type, its scope, and whether access was granted or denied.

(b) The monitoring mechanism will not enable, to the extent possible, disabling or modifying its operation; the monitoring mechanism will detect such modifications or the disabling of its operation and will send alerts to those responsible.

(c) A database controller will prescribe a routine procedure to examine the records of the monitoring mechanism, prepare a report of the issues found and the measures taken as a result.

(d) The records of the monitoring mechanism will be retained for at least 24 months.

(e) A database controller will inform the database authorized users of the monitoring mechanism to the database systems.

Documentation of security incidents

11. (a) A database controller is responsible to document every case in which an event was discovered, raising concern regarding a breach of the data integrity, unauthorized use thereof or deviation from authorization (hereinafter - "security incidents"); the said documentation will be based as much as possible on automatic records.

(b) In the data security procedure, a database controller will also prescribe instructions with respect to handling information security incidents, depending on the event severity and the information sensitivity level, including with respect to revoking authorizations and other necessary immediate measures, and with respect to the reporting of security incidents to the database controller and the actions taken in response.

(c) In a database subject to medium security level, the database controller will hold a discussion regarding data security incidents at least once a year and assess the need to update the data security procedure; in a database subject to high security level, such a discussion will be held at least quarterly.

(d) In case of a severe security incident -

(1) The database controller will immediately notify the Registrar and report to the Registrar on the measures he took following the

incident;

(2) The Registrar may order a database controller, except a controller of the databases listed in Section 13(e) of the Law, and after consulting with the head of the National Cyber Defense Authority, to give a notice of the security incident to a data subject who may suffer damage as a result of the incident.

Portable devices

12. A database controller will restrict or deny the option to connect portable devices to the database systems in a manner which is compatible with the information security level applicable to the database, the data sensitivity, the special risks to the database systems or to the data, stemming from connecting portable devices and with the existence of appropriate safeguards against such risks; a database controller who enables using data from the database on a portable device or copying the data to a portable device will take protection measures according to the special risks related to the use of a portable device in that database; in this regard, employing commonly used encryption methods will be deemed taking reasonable measures to protect the data copied to a portable device.

Secure and updated management of the database systems

13. (a) A database controller will ensure that the database systems are managed and operated properly, as commonly acceptable in the operation of such systems.

(b) A database controller will separate, to the extent and level reasonably possible, between the database systems which enable access to data and other computer systems used by the database controller.

(c) A database controller will ensure updating the database systems on a regular basis, including the computer material required for their operation; no use will be made of systems whose manufacturer does not support their security aspects, unless an appropriate security solution is provided.

Network security

14. (a) A database controller will not connect the database systems to the Internet or to another public network without installing the appropriate safeguards against unauthorized penetration or against software that can damage or disrupt computers or computer material.

(b) The transfer of information from the database through a public network or the Internet will be conducted by commonly used encryption methods.

(c) In a database that can be accessed remotely using the Internet or another public network, measures intended to identify the user and verify his permission to perform the activity remotely and the scope of such permission, will be used in addition to the safeguards pursuant to Sub-

Regulations (a) and (b); with respect to access of an authorized user to a database with a medium or high security level, a physical means subject to the exclusive control of the authorized user will be used.

Outsourcing

15. (a) A database controller entering into an agreement with an external service provider in order to receive a service which involves granting this external service provider access to the database -

(1) Will assess, prior to entering an agreement with the external service provider, the data security risks involved in the engagement;

(2) Will expressly agree with the external service provider (in this Regulation - the "agreement") on the following, taking into account the risks mentioned in Paragraph (1):

(a) The data the external service provider may process and the permitted purposes of its use as required by the agreement between the parties;

(b) The database systems that the external service provider may access;

(c) The type of processing or activities the external service provider may perform;

(d) The agreement duration, the manner of returning the data to its controller at the end of the agreement, its destruction at the disposal of the external service provider and of reporting accordingly to the database controller;

(e) The manner data security obligations which apply to the processor of the database according to these Regulations are implemented, and additional data security instructions set by the database controller, if any;

(f) The external service provider shall have his authorized users sign an undertaking to protect the information confidentiality, to use the data only according to the agreement and to implement the data security measures prescribed in the agreement as per Sub-Paragraph (e);

(g) Where a database controller permitted the external service provider to provide the service through another entity - it is the duty of the former to include in the agreement with the other entity all the matters detailed in this Regulation;

(h) The external service provider must report, at least annually, to the database controller on the manner the obligations by these Regulations and the agreement are

implemented, as well as to notify the database controller in case of a security incident;

(3) Will detail in the data security procedure of the database also the matters listed in Paragraph (2)(a) to (e) and will explicitly refer to the agreement with the external service provider and his data security procedure;

(4) Will take measures to monitor and supervise the compliance of the external service provider with the provisions of the agreement and these Regulations, as appropriate, taking into account the risks mentioned in Paragraph (1).

(b) An organization that controls several databases and enters into an agreement with an external service provider which involves access to these databases by the external service provider may comply with the provisions of Sub-Regulation (a)(2) in a single agreement concerning all databases, provided that they all have the same security level.

(c) This Regulation will not apply to an agreement between a database controller and an individual.

Periodical audits

16. (a) In a database subject to medium or high security level, the database controller is responsible to conduct, at least once in 24 months, an internal or external audit by an auditor adequately trained in the field of data security who is not the database's own data security officer, in order to ensure it complies with the provisions of these Regulations.

(b) In the audit report, the auditor will report on the adherence of the security measures to the data security procedure and to these Regulations, identify shortcomings and recommend the necessary measures to correct the situation.

(c) A database controller will review the audit reports sent to him and assess the need to update the database definitions document or the data security procedure accordingly.

(d) A controller of a database subject to high security level may fulfil the duty prescribed in this Regulation while conducting a risk assessment which complies with the provisions of Sub-Regulation (b).

(e) An organization that controls several databases may comply with the duty prescribed in this Regulation by performing a single audit for all the databases it controls which have the same security level.

Retaining security data

17. (a) A database controller will retain the data collected when implementing the provisions of Regulation 6(b), 8 to 11, 14, 15(a)(4) and 16, to the extent these Regulations apply to him, in a secure manner for 24 months.

(b) In a database subject to medium or high security level, the database controller will back up the data retained as per Sub-Regulation (a) in a manner ensuring that the data can be restored to its original form at all times.

Data backup and restoration

18. (a) In a database subject to medium or high security level, the database controller will prescribe in a document -

(1) Procedures for routine periodical backup according to Regulation 17(b);

(2) Procedures to ensure restoring of the data as per Regulation 17(b), provided that such restoration will be with the approval of the database manager;

(3) That when documenting security incidents pursuant to Regulation 11, data restoring processes will also be documented, including the identity of the person who performed the data restoration and the details of the information restored.

(b) In a database subject to high security level, the database controller is responsible to retain the backup copy of the data mentioned in Regulation (a)(1) and of the procedures as per Sub-Regulation (a)(2) in a manner that ensures the integrity of the information and the ability to restore the information in case of loss or destruction.

Obligations of a database controller apply to a database manager and processor; and documenting activity

19. (a) The obligations that apply in these Regulations to a database controller will also apply to a database manager, and with the exception of the obligations prescribed in Regulations 2 and 15(a), they will also apply to the database processor, with the necessary changes as relevant.

(b) A person who bears a duty or responsibility to perform an action required by these Regulations which is not creating a document, shall reasonably document the manner this action is performed, as relevant; the Registrar may give instructions regarding the manner of such documentation.

Registrar's powers

20. (a) (1) The Registrar, if he believes there are justified reasons, may exempt a certain database from data security obligations pursuant to these Regulations or may impose on a certain database obligations according to these Regulations, in their entirety or some of them, depending on the circumstances, and taking into account, inter alia, the size of the database, the type of information it contains, the scope of activity of the database or the number of its authorized users;

(2) Exempting from, or imposing, obligations pursuant to Paragraph (1) will take place with a written notice to the database

controller; in such a notice the Registrar will prescribe the date in which the exemption from, or imposition of, obligations, as the matter may be, will take effect and may determine different dates with respect to different regulations.

(b) The Registrar may order that those who comply with the instructions of a guidance document regarding data security or the applicable instructions issued by a competent authority with respect to data security, will be deemed to have complied with the provisions of these Regulations, in their entirety or in part, provided the Registrar is satisfied that compliance with the provisions of the guidance document regarding data security or with the applicable instructions issued by a competent authority, as the matter may be, as ordered by the Registrar in accordance with these Regulations, ensures the security level prescribed in these Regulations with respect to that database; in this regard –

"Competent authority" - a public body authorized by law to issue instructions with respect to data security;

"Guidance document regarding data security" - an official standard, Israeli standard or international standard as defined in the Standards Law 5713-1953 or a reference document approved by the Registrar in this regard.

Applicability and exemption to applicability

21. In these Regulations –

(1) With respect to databases subject to high level of security - Regulation 1 to 20 shall apply;

(2) With respect to databases subject to medium level of security - Regulation 1 to 4, 5(a), (b) and (e), 6 to 15, 16(a), (b), (c) and (e), 17, 18(a), 19 and 20 shall apply;

(3) With respect to databases subject to basic level of security - Regulation 1 to 3, 4(a), (b), (c), (e) and (f), 5(a), (b) and (e), 6(a), 7(a) and (b), 8, 9(a) and (c), 11(a) and (b), 12 to 15, 17, 19 and 20 shall apply;

(4) With respect to a database managed by an individual - Regulations 1, 2, 6(a), 9(a), 11(a), 12 to 14 and 20 shall apply.

Commencement

22. These Regulations will take effect one year after their publication.

Transitional provision

23. Notwithstanding the provisions of Regulation 7(a), with respect to those who are authorized users on the day these Regulations take effect, a database controller subject to the said Regulation shall assess their suitability to access the database through reasonable measures, commonly used in procedures for screening and placing employees, and taking into account the information sensitivity and access permission type, and will

update the access authorizations as necessary.

Revocation

24. Regulations 2, 3, 9, 10, 12, 13, 14 and 15 of the Protection of Privacy Regulations (Conditions for Data Storage and Protection and Data Transfer Between Public Bodies) 5746-1986 – are null and void.

Relation to other enactments

25. These Regulations shall apply in addition to provisions concerning data security in other enactments unless there is a conflict between them.

First Schedule

(Regulation 1 and the Second Schedule)

1. Databases subject to medium level of security -

(1) A database whose main purpose is collecting data in order to transfer it to a third party as part of regular professional activity, including direct mailing services;

(2) A database whose controller is a public body as defined in Section 23 of the Law, even if the provisions of Paragraph (1) or (3) are not complied with;

(3) A database which contains data which is one of the following:

(a) Information about a person's intimate life, including his conduct in the private domain;

(b) Medical information or information regarding the person's mental condition;

(c) Genetic information as defined in the Genetic Information Law 5761-2000;

(d) Information about a person's political opinions or religious beliefs;

(e) Information about a person's criminal records;

(f) Telecommunication data as defined in the Criminal Procedure Law (Enforcement Powers - Telecommunication Data) 5768-2007;

(g) Biometric information;

(h) Information about a person's assets, financial debts and liabilities, financial situation or a change thereof, his ability to meet financial undertakings and the extent these are met by this person;

(i) A person's consumption habits that may denote information as in Items (a) to (g) or regarding a person's personality, beliefs or opinions.

2. Notwithstanding the provisions of Item 1(3), a database that adheres to one of the following is not subject to medium security level but rather to the basic security level:

(1) The database contains information of the types listed in Item 1(3)(b), (e), (f), (g) with respect to facial photos only and (h) regarding the employees or suppliers of the database controller, provided the information is used for the sole purpose of business management and does not include information of the types listed

in Item 1(3)(a), (c), (d) and (g) with respect to information that is not facial photos and (i);

(2) There are no more than ten users authorized by the database controller.

Second Schedule

(Regulation 1)

Databases subject to high level of security -

(1) A database according to Item 1(1) or (3) of the First Schedule, including a database of a public body as defined in Section 23(1) of the Law that fulfils the provisions of Items (1) or (3) and contains information about 100,000 persons or more;

(2) A database according to Item 1(1) or (3) of the First Schedule, including a database of a public body as defined in Section 23(1) of the Law that fulfils the provisions of Items (1) or (3) and has more than 100 authorized users.

5 April 2017

Ayelet Shaked
Minister of Justice