August 5, 2024

An amendment to the Israeli Protection of Privacy Law will increase exposure for violation of data protection requirements

Client Updates

On August 5, 2024, the Knesset approved a comprehensive amendment to the Protection of Privacy Law, which will significantly increase exposure for companies for violation of data protection requirements. Amendment no. 13 to the Protection of Privacy Law, 1981 (the "**Amendment**" or "**Amendment 13**" and the "**Law**", respectively), grants extensive enforcement powers to the Privacy Protection Authority (the "**PPA**") including the imposition of financial sanctions, expands the grounds for claiming statutory damages for data protection violations, and establishes a reform in the management and registration of databases.

In this update, we have summarized the main changes included in the amendment, and the steps you should take to prepare.

What are the main changes in Amendment 13 and what is their impact on companies?

• **Obligation to appoint a Data Protection Officer (DPO)**: Entities whose main activity involves the processing of particularly sensitive data on a significant scale, including banks, insurance companies, medical institutions, credit providers, and more, will be required to appoint a Data Protection Officer. This obligation will also apply to entities whose primary activity includes regular and systemic monitoring of individuals, their behavior, location, etc. (such as cellular service providers), as well as data brokers. Public bodies and those holding databases of public bodies (for example, companies providing data storage services to public bodies) will also be required to appoint a DPO. For more details on the obligation to appoint a DPO, please read our previous update on that matter.

• **Expansion of transparency obligations in the collection of personal data**: Prior to the Amendment, database controllers were required to inform the data subject of the purpose for which personal data is collected, the third parties to whom the data will be disclosed and the purposes of the disclosure, as well as whether there is a legal obligation to provide the data. Now, controllers are also required to inform the data subject of the consequences of not consenting to the disclosure of the data, the details of the database controller, and of the rights to access and correct the data.

• **Change in basic terms**: The definition of "Personal Data" (replacing "Information") was significantly

© All Rights Reserved to Gornitzky & Co. – Israeli Law Firm

expanded to align with global privacy laws, such as GDPR and it now includes any "data related to an identified or identifiable person". Additionally, the definitions of "sensitive data" and "holder" were expanded as well, and a definition of "database controller" was added (replacing the term "database owner" which was not previously defined under the Law). Furthermore, the Amendment eliminated the concept of a "database manager", who prior to the Amendment, had personal responsibility for the security of the personal data in the database and for aspects related to its registration.

• **Expansion of the powers of the Privacy Protection PPA**: The Amendment significantly expands the powers of the PPA, including granting it the power to impose financial sanctions for violations of the Law and the regulations enacted thereunder. Such sanctions can potentially amount to millions of shekels for multiple or recurring violations. The amount of the monetary sanctions will generally be determined by the nature of the violated provision, the number of data subjects, the size of business, and the level of security applicable to the database under the Privacy Protection Regulations (Data Security), 2017 (the "**Data Security Regulations**"). Additionally, the Amendment grants the head of the PPA the power to request the court to issue an order to a controller or holder of a database to cease data processing activities that cause or may cause a violation.

• **Expansion of the grounds for statutory damages**: New grounds for granting statutory damages were added, including in the event of failure to register a database, failure to meet the disclosure requirements (see above), failure to comply with a request to access or correct information, and more.

• **Significant reduction of the database registration requirement**: Pursuant to the Amendment, the registration requirement will only apply to databases of data brokers that contain personal data of more than 10,000 individuals, and to databases of public bodies. In the case of a database containing highly sensitive information of more than 100,000 individuals, the controller will be required to notify the PPA of its existence and provide certain details about the database.

What should you do to prepare for the Amendment's entry into effect:

• **Update Privacy policies and notices**: Revise your organization's privacy policies and notices to comply with the new transparency requirements.

• **Review the classification of databases**: Organizations should assess whether datasets which were not previously considered "Databases" now fall under this definition and are subject to the provisions of the Law, considering the expansion of the term "Personal Data".

• **Appoint a Data Protection Officer**: As mentioned above, certain entities must appoint a DPO pursuant to the Amendment. However, organizations that are not subject to that requirement could also benefit from

© All Rights Reserved to Gornitzky & Co. – Israeli Law Firm

the appointment of a DPO. Such an appointment helps embed privacy principles into organizational processes, ensure compliance with privacy laws, and mitigate risks associated with personal data management. Moreover, the appointment of a DPO can enhance customers' trust in the organization's privacy practices.

• **Examine the impact of changes to database registration obligations**: Assess the impact of the changes to the database registration requirement and comply with the updated registration and notification requirements (where applicable).

• **Conduct a comprehensive review of compliance with the Law and the regulations**: Since Amendment 13 significantly increases exposure for organizations due to violations of the Law and its regulations, companies must not only implement the new requirements outlined in the Amendment but also thoroughly review their compliance with existing requirements, especially focusing on the Data Security Regulations, which have been the focus on enforcement and supervision efforts by the PPA in recent years.

Conclusion

Amendment 13 is a significant milestone in the development of privacy laws in Israel, bringing a substantial increase in exposure for companies for data protection violations. The Amendment will come into effect one year after its publication, however, companies should start preparing for the changes as soon as possible.

Our firm's Cyber and Privacy team has vast experience in advising global and Israeli companies on compliance with data protection and privacy laws. We also provide Data Protection Officer (DPO) services and conduct compliance audits for companies to identify and address gaps in meeting the requirements of the Law and regulations. For additional information on our DPO services, please read Gornitzky's DPO services overview.

We invite you to contact us for any questions and/or advice on this matter.

This client update was prepared with the assistance of Lana Haj Yahia.

- This update is intended to provide general and concise information only. It does not constitute a complete analysis of the issues discussed, does not constitute a legal opinion or legal advice, and should not be relied upon.

© All Rights Reserved to Gornitzky & Co. – Israeli Law Firm

Key Contacts

Assaf Harel
Partner

Rebecca Genis Shepetovsky
Partner

© All Rights Reserved to Gornitzky & Co. – Israeli Law Firm