January 12, 2025

Privacy Law in Israel in 2025 – 10 Steps to Navigate the Implementation of Obligations

Client Updates

2025 brings increased exposure for violation of data protection requirements for companies and organizations operating in Israel. This applies to any company holding personal data, even if such data is limited to the company's employees. That increased exposure is due to the entry into force of Amendment No.13 to the Privacy Protection Law, 1981 ("**Amendment 13**" and the "**Law**", respectively), the full implementation of the regulations concerning personal data transferred to Israel from the European Union, and the Privacy Protection Authority's ("**PPA**") guidance on the board of directors' role in implementing the organization's data security obligations.

In this client update, we have outlined **10 key steps** to ensure compliance with legal requirements and avoid financial penalties:

1. **Updating the organization's privacy policies and notices** – Amendment 13 introduces new and enhanced transparency requirements. Therefore, it is crucial to revise privacy policies and notices to meet the current transparency requirements.

2. **Appointing a Data Protection Officer (DPO)** – You should assess whether, in light of Amendment 13, you are required to appoint a DPO. Even if not legally mandated, consider appointing a DPO, particularly if your company processes significant amounts of personal or sensitive data, as it can help mitigate risks associated with personal data management and enhance trust in the organization.

3. **Notification/Registration of Databases** – Amendment 13 introduces a reform in the management and registration of databases. You should assess how Amendment 13 impacts the registration requirements relating to your organization's databases and whether the organization must notify the PPA or if there is a need to deregister existing databases.

4. **Updating database definition documents** – Every organization is required to document the characteristics of its databases, including the purpose of the data, the types of data collected, information on data transfers abroad, processors, and more. This document should be reviewed and updated at least annually or when significant changes occur.

5. **Data Minimization** – You should evaluate annually whether the data stored in the organization's

databases exceeds what is necessary for the database's purposes. For instance, data on inactive customers or former employees may no longer be needed. While minimizing excess data is important, it is also essential to retain certain types of data for legal defense or compliance purposes.

6. **Updating Data Security Procedures** – You should evaluate whether the organization's data security procedures require updating, at least annually or more frequently if significant changes occur in the database systems or data processing practices, or if new technological risks to these systems are identified.

7. **Data Protection Training** – The Privacy Protection Regulations (Data Security), 2017 ("**Data Security Regulations**") require providing privacy protection and data security training to staff members with access to personal data, upon granting new access credentials or modifying existing credentials. For databases classified as "medium" or "high" security databases, training should be conducted at least once every 24 months. It is recommended to ensure that such training is provided within the organization at least once a year.

8. **Security Incidents** – For medium and high security level databases, a discussion regarding security incidents that occurred within the organization should be held annually or quarterly, respectively.

9. **Penetration Tests and Risk Surveys** – For medium and high security level databases, risk surveys and penetration tests should be performed at least once every 18 months.

10. **Comprehensive Examination of Compliance with the Law and Regulations** – As mentioned above, Amendment 13 significantly increases the exposure for organizations due to violations of the Law and the regulations enacted thereunder. Beyond preparing for the new requirements, organizations must thoroughly examine their compliance with existing requirements, particularly the Data Security Regulations that have been the focus of the PPA's enforcement and supervision actions in recent years. Additionally, it is important to assess whether the Privacy Protection Regulations (Instructions Regarding Data Transferred from the European Economic Area to Israel), 2023, apply to the organization, and if so, ensure their implementation.

Given the developments in privacy law in Israel in 2025, particularly with the implementation of Amendment 13, companies and organizations will face significantly increased exposure to privacy and data security risks. It is crucial to prepare in advance for these changes and to diligently conduct annual checks at the beginning of the year to ensure that the organization is managing its obligations (both annual and ongoing) in an orderly and responsible manner.

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 Israeli privacy laws. For additional information on our DPO services, please read Gornitzky's DPO services overview.

Please contact us for any questions and/or advice on this matter.

This client update was prepared with the assistance of Meira Kahn.

Key Contacts

Assaf Harel
Partner

Avital Haitovich
Senior Associate