View this email in your browser

Amendment 13 to the Privacy Protection Law Is on the Horizon - Is Your Organization Ready for the New Era in the World of Privacy?

July 2025

In a few weeks - on August 14, 2025, Amendment 13 to the Privacy Protection Law, 5741-1981 will come into effect - embodying a comprehensive and fundamental reform in Israeli privacy laws.

The amendment revolutionizes the privacy law system in Israel, bringing it closer to European standards (GDPR) both in practical and terminological aspects, i.e., using parallel definitions and terms, and granting the Privacy Protection Authority extensive enforcement powers unprecedented in the field of privacy in Israel.

Accordingly, every organization - whether a company, non-profit, public body, or business that processes personal data - must **now** take steps to comply with the provisions of the amendment and mitigate the risks of enforcement actions, lawsuits, and reputational damage.

Key Changes Following Amendment 13:

- **Expansion of Supervision, Enforcement, and Fine Powers**:
  The amendment to the law grants the Privacy Protection Authority extensive and significant enforcement powers, including the authority to impose substantial financial sanctions on companies and organizations that violate the provisions of the law or the regulations thereunder. The amount of the fines may reach hundreds of thousands and even millions of NIS in severe or repeated cases. The Authority will also be able to request court orders to cease the processing of personal data and even its deletion – steps that could paralyze the

organization's activities and publicize the violation and the sanction imposed – which could harm the organization's image and reputation.

- **Expansion of Causes of Action and Compensation**:
  The authority of the courts to award exemplary damages (without proof of damage) has been expanded in a variety of cases of violation of the law, up to an amount of NIS 10,000 per violation. This means increased exposure to personal lawsuits even when no actual damage has been caused. We estimate, and are already seeing early signs of this in our ongoing activities, that the expansion of the causes of action and compensation as mentioned will be exploited by many and will lead to a wave of lawsuits, similar to the effect brought by the Spam Law.
- **Obligation to Appoint a Data Protection Officer (DPO)**:
  Many organizations in the Israeli economy will be required to appoint a **Data Protection Officer** - public bodies, companies engaged in the trade of information, companies that process sensitive personal data on a large scale, or those whose activities involve systematic monitoring of individuals. This is a new mandatory role in Israeli law, parallel to the role of the Data Protection Officer (DPO) under the European privacy regulations (GDPR). The role of the officer is to ensure compliance with the provisions of the law, promote privacy protection, serve as a professional knowledge hub, advise management and employees, supervise the implementation of procedures, handle inquiries from data subjects, and serve as a liaison with the Privacy Protection Authority. Accordingly, a legal review is necessary to determine whether the obligation to appoint a Data Protection Officer arises and, if so, who is the appropriate entity to fill the role in accordance with the requirements of the law.
- **Expansion of the Duty to Inform and Transparency**:
  The amendment expands the details that must be provided to the data subject when collecting personal data. The data subject must be informed not only of the purpose of the collection and the third parties, but also of the consequences of non-consent, the details of the controlling shareholder of the database, the rights of access and correction, and whether there is a legal obligation to provide the information or if it depends on consent. **This expansion requires updating all privacy notices and policies within the organization**.
- **Reduction of the Database Registration Obligation and Notification Obligation in Lieu of Registration**:
  The registration obligation will apply only to databases whose main purpose is the delivery of information to others for consideration, or databases of public bodies. Databases containing particularly sensitive information on more than 100,000 data subjects will be required to report the database to the Authority, including providing details of the controlling shareholder, the Data Protection Officer, and the database definition document, in lieu of registering the database. Accordingly, the status of the registration obligation for databases must be re-examined, and for databases registered in the past, the possibility of deleting the database registration should be considered.
- **New Criminal Offenses**:
  The law establishes new criminal offenses, including processing data without authorization and intentionally misleading a data subject. The penalties for these offenses can reach up to three years of imprisonment or significant fines. In addition, an explicit prohibition is established on performing any action with personal data collected in violation of the law's provisions.

  In addition, it is important for you to know that in recent months, the Privacy Protection Authority has published several significant guidelines and position papers that affect the obligations of organizations in the field of privacy protection, including:

- A guidance document on the responsibility and role of the board of directors in privacy and information security matters

- A draft guidance on the applicability of the Protection of Privacy Law to the use of artificial intelligence tools
- A draft position paper on "What is Consent" under the Protection of Privacy Law

These developments create a new regulatory environment that may affect the activities of many organizations and require preparation accordingly.

In light of this, we recommend examining the applicability of Amendment 13 and the new guidelines to your organization's activities, and considering the appropriate steps for preparation through an in-depth analysis of all processes and aspects related to the collection, processing, and storage of information in your organization, in order to avoid exposure to sanctions, lawsuits, and even criminal liability.

Meitar's privacy team is at your disposal to answer questions on the subject and to provide guidance and assistance in implementing the new requirements in relation to your organization.

Contact

Tali Yavin- Surasky, Partner
+972-3-6103998
taliy@meitar.com

Eden Abraham, Senior Associate
+972-3-6144857
edena@meitar.com

Tamir Shenhav, Associate
03-6103861
tamirsh@meitar.com

Dor Reshef, Associate
דיני פרטיות והגנת מידע
03-6144013
dorr@meitar.com

Dana Nissim, Associate
דיני פרטיות והגנת מידע
03-6103977
danan@meitar.com

For more information about our Privacy and Data Protection Law parctice, click here

---

מיתר | עורכי דין
דרך אבא הילל סילבר 16, רמת גן, 5250608, ישראל | 03-6103100