Privacy Protection Authority Guidance No. 1/2024:
The Role of the Board of Directors in Carrying out Corporate Obligations under the Privacy Protection Regulations (Data Security)

Background

1. The Privacy Protection (Data Security) Regulations, 5777-2017 (hereinafter: "the Regulations") stipulate obligations and actions that a database controller, its processor and its manager are required to perform in order to fulfill their responsibility under Article 17 of the Privacy Protection Law, 5741-1981, regarding the security of the data in the database.

2. **In a company where the processing of personal data is at the core of its activity or where it is probable that its activity will create an increased risk to privacy, the Privacy Protection Authority's position is that the board of directors is obliged to oversee the company's compliance with the Law and the Regulations, in accordance with the following principles. The board is responsible for ensuring** the establishment, adoption, and implementation of a policy regarding the manner in which the company carries out the requirements of the Law and the Regulations, including the obligation to immediately report data security breaches to the Privacy Protection Authority. The policy should address, *inter alia*, the manner in which personal data are used and managed by the company on material matters and should define an effective mechanism for supervision, monitoring, and compliance. The board must also ensure that the policy is embedded in the company's work procedures and must determine the organs responsible for its implementation. The board is responsible for the ongoing monitoring, as well as receiving updates and reports from the responsible organs on the fulfillment of the obligations under the Regulations.

3. In addition, although the Regulations do not explicitly determine the organ responsible for carrying out the obligations imposed on the company,[1] the Privacy Protection Authority's position is that in companies in which the processing of personal data is at the core of the activity or the activity creates an increased risk to privacy, the performance of certain supervisory duties further specified in Section 11 below, imposed under the Regulations on a company as a database controller or processor – should be carried out by the company's board of directors, taking into account the specific characteristics of the company.

4. This position is based on a purposive interpretation of the Privacy Protection Law and the Regulations, taking into account the principles of corporate governance and the conventional division of roles between the organs of the corporation under the Israeli Corporate Law. Article 92 of the Companies Law, 5759-1999, stipulates that "The board of directors shall outline the policy of the company and shall supervise the performance of the functions and acts of the general manager within that framework…". It is also in line with corporate case law in the United States, which is gaining traction in the rulings of the Israeli courts.

5. In the **Caremark** case,[2] the Delaware Court ruled that the board has an obligation to create internal monitoring and supervision mechanisms in the company, in order to monitor the company's compliance with all statutory provisions applicable to it. The Court held that a company's board of directors must ensure the existence of a **reasonable** internal compliance and reporting system that will provide the board with sufficient, accurate and up-to-date information, in order for it to make informed decisions regarding the company's compliance with the law. This obligation does not apply only when the board is presented with information that raises suspicion of a violation of the law. This is a general obligation, which the board must implement, as a matter of routine and in advance, internal monitoring and reporting mechanisms.

[1] Apart from a limited number of tasks which Article 3 of the Regulations expressly stipulates as the responsibility of the company's Data Security Officer.
[2] *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996). See also *Marchand v. Barnhill*, 212 A.3d 805 (Del. 2019).

6. According to this ruling, liability of the board may arise in two types of situations: First, in the case of an "utter failure" by the board to implement a mechanism for monitoring, control, or receiving information about regulatory compliance; Second, if the board has implemented such a mechanism but consciously failed to oversee its de-facto application, thus preventing the directors from knowing about risks or problems, including "red flags," which required their attention.[3] A recent ruling by the Delaware court held that in this regard, cyber security in online service providers is "mission critical" to the company.[4]

Moreover, the 2021 ruling by the Delaware Court in the case of **Marriot** hotel chain is also noteworthy.[5] The lawsuit was filed in the aftermath of a cyber-attack that resulted from a data security failure in the company's systems, which created a threat of exposure of data about hundreds of millions of the company's customers. Regarding some of these customers, the threat included the exposure of sensitive personal data, such as passport numbers. The attack led to a large-scale personal data leak, after which various criminal and civil proceedings were conducted against the company. As for the board's liability for the damage, the Delaware Court held, based on the **Caremark** ruling, that cyber and data security risks are some of the issues for which the duty of care applies:[6]

> "Delaware courts have not broadened a board's Caremark duties to include monitoring risk in the context of business decisions. Oversight violations are typically found where companies—particularly those operating within a highly regulated industry—violate the law or run afoul of regulatory mandates. **But as the legal and regulatory frameworks governing cybersecurity advance and the risks become manifest, corporate governance must evolve to address them. The corporate harms presented by non-compliance with cybersecurity safeguards increasingly call upon directors to ensure that companies have appropriate oversight systems in place**."

[3] Stone v. *Ritter* 911 A.2d 362 (Del. 2006).
[4] *Constr. Indus. Laborers Pension Fund v. Bingle,* (Del. Ch. Sept. 6, 2022).
[5] Fireman's Retirement System of St. Louis v. Sorenson et al. (Del.Ch. Oct. 5, 2021).
[6] It should be noted that in this case the Court found that the board had taken appropriate measures, and therefore held that the directors are not liable according to the duty of care. This guidance outlines the standards for such measures with regard to the duties in Israel under the Privacy Protection Regulations (Data Security), 5777-2017.

7. In recent years, corporate violations have been at the center of many lawsuits filed in Israeli courts, most of them derivative suits filed on behalf of the company, against directors, based on a negligence claim with regard to their supervision over the company's business, following fines or other sanctions imposed on the company due to violation of the law in Israel or abroad. Many of these cases ended with settlement agreements.[7] As a result, the implementation of the **Caremark** ruling in Israeli case law is yet to be determined. However, based on the Attorney General's opinion filed in the **Aharoni** case, in the Tel Aviv District Court, where similar questions arose regarding the board's duty of care and the liability of directors for the company's damage, the District Court asserted that "it seems that such ruling in Caremark that was correct and proper back in 1996 should be adopted as a proper and right standard in Israel in 2021 as well."[8]

Guidance

8. This guidance applies to companies for which the processing of personal data is at the core of their activity,[9] or to companies who their activity creates an increased risk of privacy violation. This, either due to the **characteristics of the company** (such as data brokers); due to the **type and sensitivity of the processed data**, such as the types of data listed in Article 1 in the First Annex of the Regulations, in the definition of "data with special sensitivity" in Amendment No. 13 to the Privacy Protection Law, recently approved by the Knesset,[10] or data concerning vulnerable populations such as minors; or due to **the scope of data or the number of authorized users** (see for example the amount of data subjects and authorized users that qualifies for a high level of security under the Second Annex of the Regulations).

[7] See Hamdani, Kastiel and Weisman "Derivative suits in Israel – Interim Summary and a look into the future" (2021).
[8] Derivative Suit (Tel Aviv) 17044-12-14 *Aharoni v. Bank Mizrahi Tefahot* (11 May 2021). See also the Attorney General opinion in that case, from January 2021.
[9] As opposed to data processing that is **only incidental** to the core activity.
[10] Privacy Protection Law (Amendment No. 13), 5724-2024, that was recently approved by the Knesset and will enter into force on 14 August 2025, establishes a new category of data types defined as "data with special sensitivity." This category affects the financial sanctions imposed for violations of the Law or the Regulations, the obligation to appoint a Data Protection Officer, and the requirement to notify the Privacy Protection Authority regarding large and sensitive databases.

9. The board of directors in a company for which Section 8 above applies, is required to ensure the existence of a policy for carrying out the requirements under the Regulations, including the obligation to immediately notify the Privacy Protection Authority on data security breaches. The policy will address, *inter alia*, the manner in which personal data is used and managed by the company in material matters,[11] and will define effective mechanism for supervision, monitoring, and compliance. The board must also ensure that the policy is embedded in the company's work procedures and determine which organs within the company are responsible for its implementation. The board is responsible for the ongoing monitoring, as well as receiving updates and reports from the responsible organs on the fulfillment of the obligations under the Regulations. The establishment of an effective internal compliance program is one of the ways in which the board's duty of care may be fulfilled.[12]

10. Notwithstanding the generality of the above, the Privacy Protection Authority's position is that in a company for which Section 9 applies. The board of directors is generally the appropriate organ to carry out the following duties, that are supervisory in nature, and are imposed on a company under the Regulations, as a database controller or processor:

    10.1 Conducting a discussion on the database definitions document – prior to its final approval, in accordance with Article 2(a);

    10.2 Conducting a discussion on the main principles of the company's data security procedure – prior to its final approval and designation, in accordance with Article 3(2) and Article 4(a).

[11] For comparison, see the position paper published by the Israel Directors' Association in 2022 on the topic of "The Board's Responsibility in the Field of Cybersecurity." See especially Annex A of the position paper, which includes selected topics that should be discussed by the board, and Annex C, which provides an example of guiding principles for an internal enforcement program.

[12] See Itai Mashiach & Zvi Gabbay, "Internal Enforcement Programs: On the Challenges Facing the Israeli Regulator," 12 Corporations 9 (2012). Compare also: "Criteria for Recognition of an Enforcement Program in the Field of Securities and Investment Management," published by the Israel Securities Authority (2011). The criteria are available in Hebrew here.

10.3 Conducting a discussion on the results of the risk evaluation and penetration tests, including the necessary corrective actions for the defects found, in accordance with Articles 5(c) and 5(d);

10.4 Conducting a quarterly or annual discussion, depending on the security level of the database under the Regulations, on data breaches that occurred in the company, in accordance with Article 11(c);

10.5 Conducting a discussion on the periodic audit reports on compliance with the Regulations, which must be held every two years, in accordance with Article 16(c).

11. However, in appropriate cases while taking into account the degree of privacy risks involved in the company's activity, its size, and the composition of the board, the board may designate a different organ within the company to be responsible for carrying out these duties, while supervising their de-facto implementation. In accordance with Article 19 of the Regulations, the board is required to ensure that its reasoning for such decision is documented in a reasonable manner and so is the implementation of other necessary actions under the Regulations.

12. This guidance does not exempt or reduce the responsibility of the CEO, the management of the company, or any other organ authorized to carry out the duties imposed by the Regulations, under the company's articles of association or under any law.