Gross Orad Schlimoff & Co.
Incorporated Law Firm

7 Menachem Begin Rd.
Ramat-Gan 5268102, Israel
Tel: 972-3-6122233
Fax: 972-3-6123322
Web Site: www.goslaw.co.il

New Guidelines of the Privacy Protection Authority regarding the Board of Directors' Oversight Duty Over Cyber Security Matters

The Israeli Privacy Protection Authority published new guidelines listing the duties of a company's board of directors in supervising the company's compliance with data security regulations, as part of the Board's oversight duty.

The Privacy Protection (Information Security) Regulations impose a series of duties and actions imposed on companies that hold or process a personal information database, in order to fulfill its responsibility under the Privacy Protection Law, regarding data security of the database.

The guidelines state that in companies whose core of business includes processing of personal information, or companies whose activity creates an increased risk to privacy, the board of directors is the appropriate organ to set out the company's policies and procedures relating to data security, and inter alia carry out the following duties, which are supervisory in nature, as stipulated in the regulations: (i) approval of the main principles of the organizational data security procedure; (ii) approval of the database definitions document; (iii) holding a discussion at the board of directors on the results of risk surveys and the results of penetration tests that the company is obligated to conduct, in accordance with the security level of its databases pursuant to the regulations and approving the actions required to rectify deficiencies which are found; and (iv) holding a quarterly or annual discussions at the board level on data security events that occurred in the organization and holding a Board discussion on the results of a periodic audit regarding the organization's compliance with the regulations, which should be held every two years.

In accordance with the guidelines, in the appropriate cases, considering the degree of privacy risk involved in the company's activity, its size and the composition of the board of directors, the board may determine that another position holder within the company will be responsible for the performance of these duties, while the board continues to supervise their performance. In such cases, the board of directors must ensure that the reasons for this decision are reasonably documented, as well as the manner of carrying out the other actions required according to the regulations.

The guidelines also state that the board of directors will determine who is responsible within the company for carrying out the requirements of the regulations, including the obligation to immediately report to the Privacy Protection Authority of data security incidents.

The board will also be responsible to implement processes of supervision, control, compliance and reporting on the implementation of the regulations by those responsible, and will also set the policy regarding the use of personal information in the company and its management in material matters.

As mentioned, the guidelines apply to companies that processing of personal information is at the core of their activity and to companies whose activity creates an increased risk to privacy. Indications for this can be the characteristics of the organization (such as companies engaged in data trading), the type of personal information processed by the organization and its sensitivity, the scope of the personal information or the number of authorized persons with access to it.

The guidelines further clarify that they shall not exempt or reduce the liability imposed on the company's CEO, the company's management, or any other organ authorized by it to carry out the duties in accordance with the regulations.

It should be noted that, during 2023, the Israel Securities Authority (ISA) published an amended position regarding disclosures required by publicly traded corporations on cyber related issues. The Israel Securities Authority's position emphasizes that the board's involvement has great weight and importance in the oversight of the company's cyber risks and data security. The position also determines that the corporation is required to report and detail its cyber risk management policy and strategy and the resources allocated for its risk management in its public reports.

GOS Comments:

The new regulatory circular aligns with the European data breach regulations and marks a crucial step toward strengthening the protection of sensitive data held by companies, especially in light of the rising cyber threats globally and in Israel. The increasing number of cyber-attacks, coupled with the evolving nature of cyber risks, has made robust data security measures more critical than ever. These heightened regulatory obligations not only serve to improve corporate data security practices but also increase the accountability of directors and officers. Failure to ensure compliance with these requirements may expose them to derivative and class action lawsuits, reinforcing the importance of diligent oversight in safeguarding company data and meeting regulatory standards.

Contact persons:
Sigal Schlimoff Rechtman, Adv. – Sigal@goslaw.co.il
Omer Shalev, Adv. – Omer@goslaw.co.il
Maya Solomon, Adv. – Maya@goslaw.co.il

Gross Orad Schlimoff & Co.
7 Menachem Begin Rd.
Ramat-Gan 5268102, Israel
Tel: 972-3-6122233
Fax: 972-3-6123322
Web Site: www.goslaw.co.il