יוני 17, 2026

National Cyber Defense Bill

Client Updates

On June 8, 2026, the Israeli Knesset approved the first reading of the National Cyber Defense Bill, 5786-2026 (link in Hebrew) (the "**Proposed Bill**"). This marks a significant step toward broad, comprehensive regulation of cyber defense in Israel, for the first time through dedicated legislation. The Proposed Bill is intended to ensure the continuous and secure functioning of the national cyberspace as part of the resilience and security of the State of Israel, while establishing tailored arrangements with respect to essential organizations and providers of digital and hosting services. The Proposed Bill adopts a tailored approach, customizing obligations and their implementation based on the organization's characteristics, the sector in which it operates, and the associated risk level.

In this update, we have summarized the key aspects of the Proposed Bill, its main implications for businesses, and the steps companies should already be taking to prepare.

Who may be affected by the Proposed Bill?

The framework outlined in the Proposed Bill focuses, but is not limited to, "essential organizations". An organization qualifies as essential if it is a government entity or if it operates within one of the sectors listed in the Third Schedule of the Proposed Bill and meets the specified sector criteria, which generally depend on the nature of the organization's activities, the scope of its operations, and the significance of the services it offers. The sectors targeted by the Proposed Bill include, among others, communications, energy, healthcare, transportation, food and essential product and service supply, as well as digital and hosting services. Providers of digital and hosting services to include, among others, certain software and technology service providers, service providers that manage and operate computer systems, data processing, cyber defense, and hosting infrastructure.

An essential organization that complies with the standards and requirements set out in its Seventh Schedule of the Proposed Bill, e.g., implementation of NIST SP 800-53 requirements, and that submits an appropriate affidavit and documents, to benefit from an exemption from some of the obligations imposed on an essential organization.

The main obligations that will apply to organizations

- **General cyber defense duty.** The Proposed Bill mandates that all organizations, regardless of whether they are classified as "essential," must implement reasonable cyber defense measures in their operations. These measures should align with the nature of their activities and the

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

associated risk levels. When evaluating the adequacy of these measures, factors such as the type and extent of computer use, the sensitivity of the information stored, potential cyber risks, and the possible damage to the organization, the public, or third parties should be considered, as well as the economic burden of implementing protective measures relative to the organization's resources and typical practices among similar entities.

- **Duty to maintain a basic level of cyber defense for essential organizations.** Alongside the general duty, the Proposed Bill requires essential organizations to maintain a basic level of cyber defense in accordance with requirements outlined in Part A of the Fourth Schedule.

These requirements encompass cyber risk management, cyber asset mapping, preparedness for cyber incidents, operational continuity, reporting mechanisms for cyber incidents or suspicions, supply chain risk management, and internal governance related to cyber defense.

- **Duty to report a significant cyberattack.** An essential organization that detects a significant cyberattack must report it to the Israel National Cyber Directorate and its supervising regulator. A "significant" attack is one that disrupts, or could potentially disrupt, the service's availability, continuity, or reliability; jeopardizes a major information asset or leads to unauthorized access; or is unlikely to be confined to the organization alone.
- **Urgent instructions to prevent a significant cyber risk.** When a cyber risk may enable a severe cyberattack against essential organizations or through them, the Proposed Bill authorizes the Head of the Israel National Cyber Directorate to instruct an essential organization in writing to take urgent measures to address the risk.
- **Documentation, record retention, and protection of personal information.** The Proposed Bill not only outlines operational requirements but also mandates the retention of documents demonstrating compliance. This includes proof of adherence to the minimum cyber defense standards and the implementation of urgent directives aimed at preventing significant cyber risks. Personal data obtained from organizations pursuant to the powers accorded by the Proposed Bill will be protected under confidentiality obligations, and its processing will align strictly with cyber defense needs. Such data will be kept only as long as necessary and will be deleted within two years unless a specific reason calls for extended retention.

Supervisory and intervention powers

The Proposed Bill grants designated authorities supervisory and enforcement powers to verify compliance with its provisions. These include allowing an authorized employee to request information and documents, such as copies of computer data, from any relevant party to ensure compliance with the law. Additionally, the employee may enter the organization's premises to monitor compliance with cyber defense obligations and reporting requirements for significant cyberattacks. In the event of a severe cyberattack, the Proposed Bill empowers the authority to issue directives to an organization to detect, prevent, or contain the attack. This can involve requesting information or documents and, in certain cases, executing cyber defense

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

actions on computer data. While these powers primarily target essential organizations, they may also extend to digital or hosting service providers during such severe attacks, even if these are not classified as essential organizations.

Financial sanctions, publication, and criminal liability

The Proposed Bill includes an administrative enforcement mechanism centered on significant financial sanctions for breaches of various obligations. Sanctions for most violations amount to NIS 640,000. Organizations may face multiple sanctions for several violations, including doubled fines for repeated violations. This sanctions framework mainly targets essential organizations that fail to meet their obligations, such as reporting a major cyberattack timely and properly, or providing necessary information and documents.

Personal liability of executives

The Proposed Bill assigns personal supervisory responsibility to corporate officers. An officer must diligently supervise and do everything possible to prevent violations relating to inadequate measures and non-compliance with instructions; failure to fulfill this duty could result in a personal fine. Additionally, the Proposed Bill states that if the corporation or its employees commit an offense, it is presumed that the officer breached their supervisory duty unless they prove they took all reasonable steps to prevent it. This presumption emphasizes the importance of senior management to actively and clearly document their involvement in managing cyber risks.

What should companies do to prepare

The Proposed Bill has not yet been approved and may still undergo changes during the legislative process.

However, companies should begin preparing by implementing the following steps:

- **Assess whether the company constitutes an "essential organization":** As noted, this definition is central to the applicability of many of the provisions under the Proposed Bill.
- **Identification and reporting mechanisms:** Essential organizations should ensure that internal reporting mechanisms are in place to enable rapid identification of a reportable incident and compliance with the short timelines prescribed by the Proposed Bill.
- **Standards and certifications:** Companies should examine whether they hold recognized standards that may assist in meeting the requirements of the Proposed Bill, or alternatively, whether they may benefit from a carve-out from some of the obligations by submitting an affidavit confirming compliance with cybersecurity standards.
- **Document retention:** Companies should ensure that there is an orderly mechanism for retaining

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

documents evidencing their implementation of cyber defense requirements, including procedures, risk assessments, decisions, remediation actions, and incident documentation.

- **Corporate governance and cyber defense:** Cyberattacks expose companies to operational and legal risks, as well as reputational risks. If adopted, the Proposed Bill is expected to increase these risks and may also expose officers of companies to personal liability for failure to comply with their supervisory obligations regarding the implementation of the Proposed Bill's requirements. Officers of the company, including senior management and members of the board of directors, should demonstrate active involvement in managing the company's cyber risks and ensure that appropriate corporate governance is in place in this area. This is particularly important for essential organizations and providers of hosting services or digital services.
- **Compliance gaps:** Essential organizations should examine the gaps between the Proposed Bill's requirements and their existing practices and procedures, and act to address them as soon as possible.

Our firm's Cyber and Privacy Group advises a wide range of companies and organizations on reducing legal exposure from cyber risks and implementing applicable regulatory requirements.

We invite you to contact us with any questions or to consult with us on this topic.

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

Key Contacts

Assaf Harel
Partner

Rebecca Genis Shepetovsky
Partner

Rona Tal
Intern

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