December 3, 2023

New Cyber Regulations Relating to the War in Gaza

Client Updates

On November 27, 2023, the Government of Israel issued new emergency regulations granting new authorities to the National Cyber Directorate and additional agencies to instruct providers of digital services or storage services to detect, prevent, and contain cyber-attacks.

The Emergency Regulations (Iron Swords) (Handling Serious Cyber Attacks in the Digital and Storage Services Sector), 2023 (the "**Regulations**") were published simultaneously with a memorandum of law containing similar provisions (the "**Memorandum**"). Once approved by the Knesset, the Memorandum is intended to replace the Regulations. These measures are a response to the significant rise in the frequency and intensity of cyber-attacks aimed at disrupting the Israeli economy. Additionally, it is noted that in recent years, the Government has taken steps to advance the Cyber Bill, which aims to provide extensive authority to the National Cyber Directorate in connection with the prevention of widespread cyber-attacks.

1. To whom do the Regulations apply?

The Regulations and the Memorandum apply to those who provide one or more of the following services ("Suppliers"):

1. data storage, data processing, and infrastructure for processing or storing data;
2. software services, including writing, adaptation, modification, testing, support, research and development;
3. management or operation services of computer systems that combine software and communication technologies;
4. data processing, input or recovery services, computer installation and configuration, software installation or cyber protection services;
5. computer supply, installation, and control equipment that are part of machinery and industrial equipment;
6. maintenance, management, or control services in relation to one or more of the services listed above.

According to the Memorandum, companies offering the aforementioned services are typically characterized by having a high level of connectivity to various entities, including government ministries, public entities, security bodies, critical infrastructure, and other organizations that are essential for the Israeli economy. Such level of connectivity enables an attack on one company to potentially inflict damage that ripples

across other companies within the economy. Therefore, in connection with the services listed in sections 1-5 above, there must be a physical or logical connection, either permanent or temporary, or a frequent transfer of information from the Supplier's computers to the computers of the service recipient, for the Regulations to apply.

2. What are the primary implications of the Regulations?

According to the Regulations, a qualified employee of the National Cyber Directorate, Israeli Security Agency, or the Director of Security of the Defense Establishment at the Ministry of Defense may inform a Supplier of an actual concern regarding a "serious cyber-attack" and demand a report from the Supplier on the actions taken to detect, prevent, or contain the attack. Alternatively, the Supplier may submit a statement demonstrating its compliance with the NIST 800-53 standard, which is a cyber-security standard of the US National Institute of Standards.

In the event that a Supplier failed to comply with the requirements and has not provided a statement, the authorized employee may instruct the Supplier on actions to be performed in computer materials or information to be provided to the authorized employee. This, after giving the Supplier an opportunity to voice its claims.

3. Are instructions issued under the Regulations subject to a right of appeal?

Appeals against decisions made under the Regulations can be filed with the Court of Administrative Affairs, as also proposed in the Memorandum.

4. When will the regulations go into effect?

The Regulations are in effect and shall remain in effect until December 26, 2023. Pending approval, the Memorandum shall supersede the Regulations and shall remain valid until one month following the expiration date of the Minister of Defense's off.

Please feel free to contact us with any questions that you have on this matter.

This client update was prepared with the assistance of Melisa Poiron.

Key Contacts

Assaf Harel
Partner

Linor Vertnik
Associate