March 2020

GORNITZKY
80 Years of Excellence

Israeli Data Protection Requirements Regarding Work from Home

Reading time: 1 minute

In light of the outbreak of the SARS-CoV-2 virus (hereinafter – "**Coronavirus**") and following the publication of restrictions by the Israeli Ministry of Health, many companies and organizations have asked their employees to work from home. Encouraging employees to work from home can facilitate business continuity in these challenging times, but can also expose the organization to cyber-security and regulatory risks.
In this update, we will address the **primary requirements** that apply, under the Privacy Protection Regulations (Data Security), 5777-2017 (hereinafter – "**Regulations**"), to remote work. We note that the Regulations apply to any database that contains personal data (such as data on the company's employees, its customers, etc.) (hereinafter – "**Database**"), and therefore are applicable to most companies.

Under the Regulations, companies should apply the following requirements for securing connections to any Database and to the systems that are used by the Database:

1. Avoid connecting systems used by the Database to the Internet or to any other public network without installing appropriate safeguards against unauthorized penetration or malicious software (e.g., installing a firewall or antivirus).
2. Use commonly accepted encryption methods when transferring personal data through the Internet (or any other public network).
3. For any Database that can be accessed remotely – apply measures for identifying users using a remote connection and for verifying their permissions. Where the Database is classified, under the Regulations, as having a “Medium” or “High” security level, a physical means under the exclusive control of the authorized user (such as smart card) should also be used.

In that context, we note that the Israel National Cyber Security Directorate has recently issued Recommendations for Working from Home in Light of the Outbreak of the Coronavirus. The purpose of these recommendations is to reduce cyber risks emanating from the increase in remote work.

An increase in work from home can expose companies to cyber-security risks that can endanger the company's business continuity and create legal exposure. Companies should implement appropriate cyber-security measures to address these risks and to comply with applicable legal requirements. This is especially important these days, where we are seeing a sharp rise in the number of cyber-security attacks on organizations in light of the Coronavirus outbreak.

Gornitzky's Cyber-Security and Privacy team is at your service should you require any clarifications or assistance.

For further information please contact:

Assaf Harel, Partner
assafh@gornitzky.com

Astar Shechter, Associate
astars@gornitzky.com