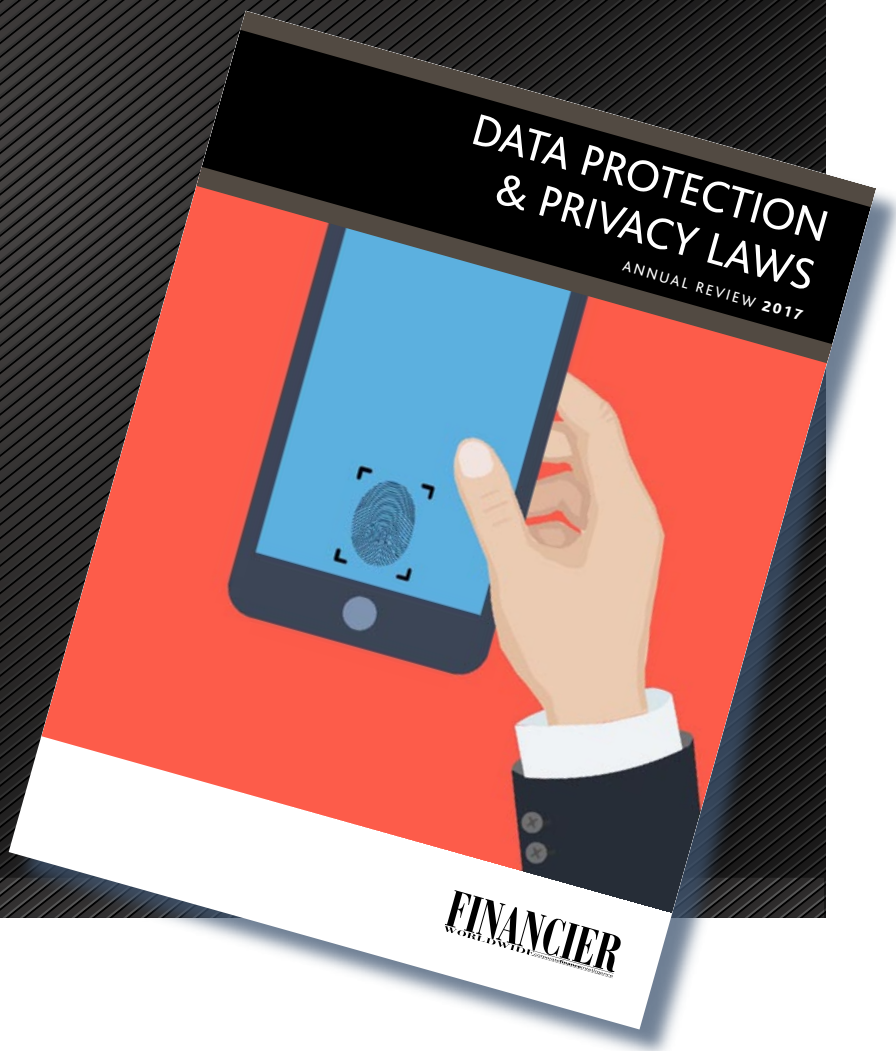
REPRINT FINANCIERWORLDWIDE.COM

ANNUAL REVIEW

Data protection & privacy laws



REPRINTED FROM
ONLINE CONTENT
NOVEMBER 2017

PREPARED ON BEHALF OF

PEARL COHEN

FINANCIER WORLDWIDE corporatefinanceintelligence

ISRAEL

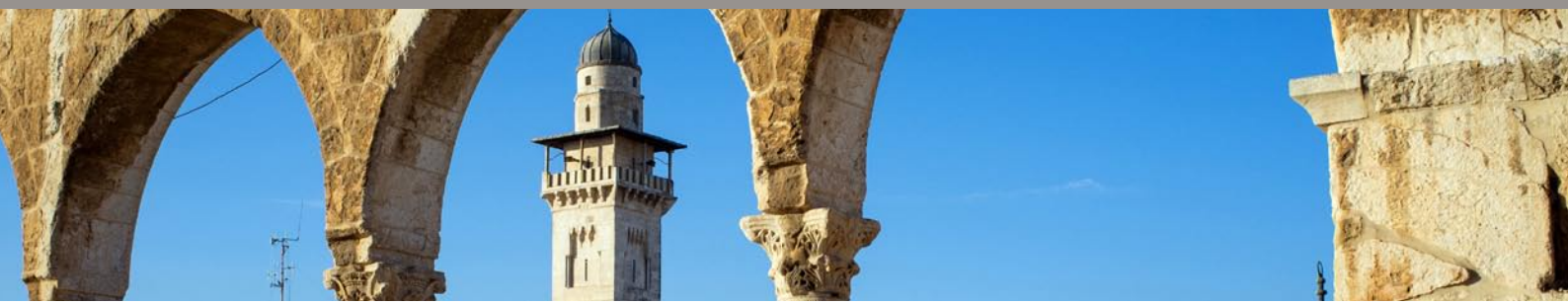
HAIM RAVIA
PEARL COHEN

Q DO YOU BELIEVE COMPANIES FULLY UNDERSTAND THEIR DUTIES OF CONFIDENTIALITY AND DATA PROTECTION IN AN AGE OF EVOLVING PRIVACY LAWS?

RAVIA: It would be presumptuous to say that companies, across the board, fully understand their data protection duties. Companies that face international clientele and that are exposed to foreign data protection and privacy laws usually exhibit an appreciable effort to comply with the evolving data protection and privacy laws, particularly the forthcoming European General Data Protection Rule (GDPR) and comparable sector-specific laws, such as the US Children's Online Privacy Protection Act (COPPA). They do so mainly because they understand that they must take steps toward compliance in order to survive in the competitive landscape in which they operate. As a result, those companies are more mindful of their duties regarding confidentiality and data protection in an age of evolving privacy laws. Likewise, companies operating within the local market also exhibit an appreciable effort to comply with the evolving Israeli data protection laws, mostly where they face larger and more sophisticated clients that demand this.

Q AS COMPANIES INCREASE THEIR DATA PROCESSING ACTIVITIES, INCLUDING HANDLING, STORAGE AND TRANSFER, WHAT REGULATORY, FINANCIAL AND REPUTATIONAL RISKS DO THEY FACE IN ISRAEL?

RAVIA: Over the past year, Israel's privacy regulator, the recently renamed Privacy Protection Authority, has been engaging in more proactive enforcement and regulatory activity. The regulator is vested with statutory authority to conduct announced or unannounced audits at premises where databases are administered, collect evidence and seize computers. Enforcement activities made public recently have dealt with data breaches associated with violations of the statutory duty to employ information security measures, violations of duties regarding direct mailing activities and the use of databases for purposes inconsistent with their registered purpose. In addition, a number of enforcement activities were taken against unlawful dealings in personal data, such as trafficking of personal health information unlawfully obtained from hospitals and healthcare providers. That said, the main financial and reputational risks facing companies in the region are similar to those of other regions – liability for damages and fines for non-compliance, costs of remediation, customer dissatisfaction and loss of consumer trust.



Q WHAT PENALTIES MIGHT ARISE FOR A COMPANY THAT BREACHES OR VIOLATES DATA OR PRIVACY LAWS IN ISRAEL?

RAVIA: Violation of the Israeli Protection of Privacy Law (PPL) is considered a civil tort. Available remedies include actual damages for proven injury or harm, injunctions, and statutory damages in an amount up to approximately US$34,000. Certain data protection related misconduct is a strict liability offence under the Israeli PPL, punishable by imprisonment for up to one year. These misconducts include, for example, using a database for purposes other than its registered purpose. Administrative fines of up to approximately US$6500 are also imposable under Israeli law for violations of the PPL's data protection regime. Continuous violations following a cease and desist letter from the Israeli regulator can increase the fine by an additional 10 percent for each day during which the violation continues. Finally, most forms of invasion of privacy under the PPL's privacy regime can also give rise to a criminal offence, punishable by up to five years in prison.

Q WHAT INSIGHTS CAN WE DRAW FROM RECENT CASES OF NOTE? WHAT IMPACT HAVE THESE EVENTS HAD ON THE DATA PROTECTION LANDSCAPE?

RAVIA: The number of notable cyber security cases made public is rather limited. Many cases are kept under the radar, yet a sizeable number of ransomware incidents have emerged which have resulted in considerable harm being done. Fraud-based misconduct has caused damage to a number of Israeli companies in the range of hundreds of thousands of dollars up to a few million dollars, mostly around those companies' international activities. As of May 2018, new Israeli data security regulation will take effect – the regulation has been coming since 2010. The emerging attention paid to cyber security has driven the consummation of this regulation to final promulgation. Drawing from experience in cyber security incidents, the new regulation imposes more stringent requirements on database owners, the most notable of which is a data breach notification requirement introduced for the first time as a non sector-specific requirement in Israeli law.

Q IN YOUR EXPERIENCE, WHAT STEPS SHOULD A COMPANY TAKE TO PREPARE FOR A POTENTIAL DATA SECURITY BREACH, SUCH AS DEVELOPING RESPONSE PLANS AND UNDERSTANDING NOTIFICATION REQUIREMENTS?

RAVIA: First, companies should appoint a chief information security officer (CISO) to oversee all information security matters in the organisation. For medium and large enterprises, it is also advisable to assemble a dedicated and trained cyber incident response team (CIRT). One key component in a data breach response plan is data breach notifications. The CIRT, with legal counsel, should determine whether statutory or contractual data breach notifications requirements are triggered in respect of the incident and accordingly prepare and implement a communication plan to provide such notifications. For improved preparedness, the analysis of required notifications should be performed ahead of time, rather than at the time of an incident. Additionally, relevant issues to consider in a response plan are procedures and plans for disaster recovery, which must also be established ahead of time, including preservation of evidence, PR involvement, the effects of the company's contractual obligations to its customer and its service provider's obligations to it and prudent invocation of cyber insurance coverage. Importantly, the company's procedures and plans should be taught, practiced and re-evaluated regularly.

Q WHAT CAN COMPANIES DO TO MANAGE INTERNAL RISKS AND THREATS ARISING FROM THE ACTIONS OF ROGUE EMPLOYEES?

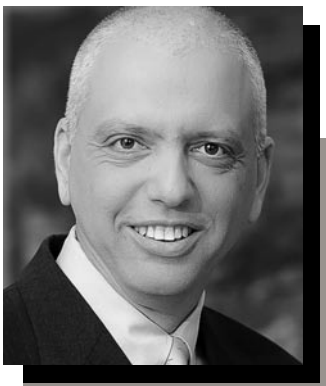
RAVIA: First and foremost, companies should adhere to traditional and long-established information security principles. These include the principle of least privilege, which requires each user only be given access to the information and computing resources strictly necessary for his or her role. Similarly applicable is the principle of data minimisation, which requires that data collection and retention be limited in the first place to what is necessary in relation to the purposes it is processed for. Ultimately, data leak detection and prevention tools are likely one of the most efficient means of managing internal risks and threats arising from the actions of rogue employees. Where these tools are too costly, invasive or pose legal compliance issues, then ongoing monitoring, particularly automated monitoring and logging of data access activities, coupled with tools for detecting access anomalies, can help prevent risks of unauthorised access and use of data.

"For improved preparedness, the analysis of required notifications should be performed ahead of time, rather than at the time of an incident."

Q WOULD YOU SAY THERE IS A STRONG CULTURE OF DATA PROTECTION DEVELOPING IN ISRAEL? ARE COMPANIES PROACTIVELY IMPLEMENTING APPROPRIATE CONTROLS AND RISK MANAGEMENT PROCESSES?

RAVIA: Sectors that are heavily regulated, such as banking and financial services, have developed a culture of data protection, mainly due to regulatory directives and oversight. In addition to this sectoral approach, the Regulation of Security in Public Bodies Law authorises the Israeli Security Agency to issue binding directives to organisations operating critical infrastructures on matters related to information security and cyber security, and inspect such organisations' compliance with those directives. Organisations subject to this regime include telecom and internet providers, Israel Railways, the Israel Airports Authority, the Tel Aviv Stock Exchange and utility companies. It should be noted that in many respects, the Israeli economy faces material cyber security risks not from individuals or organised crime in the traditional sense, but rather from actors that are sponsored by state adversaries such as Iran, China and the Russian Federation or by terrorist organisations such as Hezbollah and Hamas.

PEARL COHEN



www.pearlcohen.com

Haim Ravia

Senior Partner
Pearl Cohen Zedek Latzer Baratz
+972 3 303 9058
hravia@pearlcohen.com

Haim Ravia deals extensively with data protection and privacy, cyber and internet law, copyright, electronic signatures and open source software. Representative matters that Mr Ravia has handled include: counselling a multinational technology corporation on Israeli privacy and data protection law applicable to collecting employee-created emails for use in US litigation; advising a major Israeli financial institution on the legal restrictions under data protection laws applicable to the migration of its data operations to an outsourced cloud solution; and counselling an Israeli public institute on the privacy law implications of its proposed project to digitise its voluminous physical archives.

www.financierworldwide.com