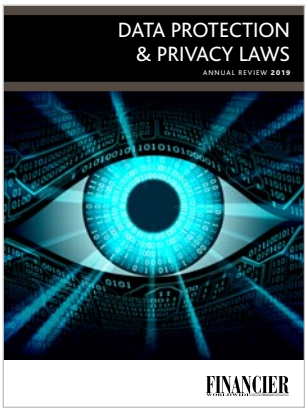

PEARL COHEN

Published by Financier Worldwide Ltd

ANNUAL REVIEW Reprint December 2019

Data protection & privacy laws

Financier Worldwide canvasses the opinions of leading professionals around the world on the latest trends in data protection & privacy laws.

Israel

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

Haim Ravia is a senior partner and chair of the internet, cyber and copyright practice group at Pearl Cohen Zedek Latzer Baratz. Mr Ravia deals extensively with data protection and privacy, cyber and internet law, IT contracts, copyright, electronic signatures and open source software. Mr Ravia was a member of the Israeli public commission for the protection of privacy and was part of a governmental team that re-examined the Israeli law pertaining to personal information databases. Practicing internet and cyber law for over 20 years, he has also written numerous columns on internet law and operates Israel's first legal website.

Q. Do you believe companies fully understand their duties of confidentiality and data protection in an age of evolving privacy laws?

RAVIA: Media and industry coverage of two pieces of legislation that took effect in May 2018 have raised awareness of data protection issues among Israeli companies. The first, the Protection of Privacy Regulations (Data Security), set out detailed and prescriptive information security requirements for all companies processing personal data. Although the Israeli privacy regulator is currently experiencing organisational instability, the effect of the new regulations has not subsided. The second piece of legislation is the EU General Data Protection Regulation (GDPR), the extraterritorial reach of which affects many Israeli companies. Awareness within companies was further reinforced recently with the Israeli government laying down a proposal for a Cyber Defence and National Cyber Directorate Bill, which aims to establish a national body whose objective is to safeguard against cyber threats. Furthermore, the looming California Consumer Privacy Act (CCPA), with its extraterritorial effect, is also elevating awareness of data protection.

ISRAEL • HAIM RAVIA • PEARL COHEN ZEDEK LATZER BARATZ

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: The financial risks are limited. First, the Israeli privacy regulator is only authorised to impose smaller penalties in limited circumstances. Second, regulatory fines are not enforceable in cases of data breaches resulting from an organisation's failure to implement the data security safeguards required under the Israeli data security regulations. Legislative attempts to improve the enforceability of the Protection of Privacy Law and the Data Security Regulations have been unsuccessful to date. The main financial risk arises from class action lawsuits, but these are not yet widespread and usually do not survive through to final judgment. That said, regulatory oversight of a company can be a painful process. The regulator can seize documents and digital evidence, investigate personnel and issue an investigative report that the company must face and address. The regulator's primary enforcement tool lies in publicly disclosing investigations, findings and conclusions about an organisation. This, in turn, can result in reputational damage that can often be more severe than other public disclosures of data breach incidents.

Q. What penalties might arise for a company that breaches or violates data or privacy laws in Israel?

RAVIA: Administrative fines of up to approximately US$6500 are imposable under Israeli law for violations of the Israeli privacy law's data protection regime. Continuous violations following a cease and desist letter 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 law's privacy regime can also give rise to a criminal offence punishable by up to five years in prison. However, under the current regime in Israel, no regulatory fines are imposable in cases of data breaches resulting from an organisation's failure to implement the data security safeguards required under the Israeli data security regulations, and regulatory enforcement powers are quite limited. Attempting to resolve this, the Israeli privacy regulator sought to advance an amendment to the law that would grant the regulator greater and more expansive

enforcement powers, including civil penalties of up to $230,000. Yet no progress was made, and this bill effectively has been abandoned.

Q. What insights can we draw from recent cases of note? What impact have these events had on the data protection landscape?

RAVIA: Once the data breach notification requirement took effect in May 2018, most data security incidents are detected and reported by information security researchers and 'white hat' hackers. Yet even under the new data breach notification regime, the negligible number of reported breaches suggests that many go unnotified. According to the Israeli privacy regulator's annual report, it carried out 146 instances of administrative enforcement action against organisations in relation to data breaches classified as 'severe'. However, the regulator was only notified of 103 of these breaches. The remaining 43 breaches were investigated after the regulator either received complaints about them or proactively discovered them. There have been very few reports of meaningful 'black hat' hacker or state-sponsored data breach incidents against commercial companies. In one recent instance, an employee of an Israeli offensive cyber security company misappropriated the company's offensive cyber tools and attempted to sell them for tens of millions of dollars on the 'darknet'. He was apprehended, indicted and convicted in a plea-bargain.

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 and foremost, cyber security breaches are a matter for the company's executives to address. The board of directors must be involved in policymaking, annual reviews and the discussion of extraordinary incidents. The company's management needs to implement the appropriate policies for handling data breaches. A data breach response procedure and policy should be established, and importantly, periodically trained on in a simulated exercise of a data breach incident. Employees should be trained to identify and decline phishing attempts. The company should map out, in advance, its reporting obligations to outside parties in case of a breach. This includes regulators, business customers, data subjects and insurance carriers.

Q. What can companies do to manage internal risks and threats arising from the actions of rogue employees?

RAVIA: This is a difficult issue facing organisations and one that calls for a diversified approach. This includes proper data security awareness training, proper HR screening and evaluation and enhanced access controls, such as physical access tokens. All of these contribute significantly to reducing these risks and are required by Israeli data security regulations. Organisations dealing with particularly sensitive information should consider using systems to monitor emails and other transmissions, leaving the organisation to reduce the risk of data leaks or breaches.

"Even under the new data breach notification regime, the negligible number of reported breaches suggests that many go unnotified."

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: Data protection culture is continuously and steadily developing. This is largely due to the surrounding ecosystem that raises awareness across companies: press reports about data breaches, class action suits alleging the data protection violations, regulatory requirements and guidelines, developments in data protection legislation, the marketing of cyber insurance policies, and more. Companies' radically differ in the proactive steps they take on cyber security, depending on factors such as company maturity, size, industry, perceived sensitivity of data and experience with breaches or cyber threats. The Israeli data security regulations require most companies to proactively implement appropriate controls and risk management processes, yet as with every law, the level and scope of compliance with the regulations is far from perfect.

www.pearlcohen.com

PEARL COHEN

HAIM RAVIA
Partner
+972 3 303 9058
hravia@pearlcohen.com

TAL KAPLAN
Partner
+972 3 303 9164
tkaplan@pearlcohen.com

DOTAN HAMMER
Partner
+972 3 303 9037
dhammer@pearlcohen.com

Pearl Cohen Zedek Latzer Baratz is an international law firm with offices in the US, Israel and the UK. The firm primarily represents innovation-driven enterprises, including Fortune 500 and small-cap emerging companies, start-ups and entrepreneurs, investors in the enterprises they form, academic institutions and government-related entities. Pearl Cohen represents clients in the areas of intellectual property, commercial law and litigation. Professionals from all of the firm's offices work together seamlessly to provide integrated legal advice covering US, Israel and certain aspects of European and Eurasian law.