DATA PROTECTION & PRIVACY LAWS

ANNUAL REVIEW **2018**

FINANCIER WORLDWIDE corporatefinanceintelligence

Published by
Financier Worldwide
23rd Floor, Alpha Tower
Suffolk Street, Queensway
Birmingham B1 1TT
United Kingdom

Telephone: +44 (0)845 345 0456
Fax: +44 (0)121 600 5911
Email: info@financierworldwide.com

www.financierworldwide.com

Annual Review • December 2018
Data Protection & Privacy Laws

DATA PROTECTION & PRIVACY LAWS

DECEMBER 2018 • ANNUAL REVIEW

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

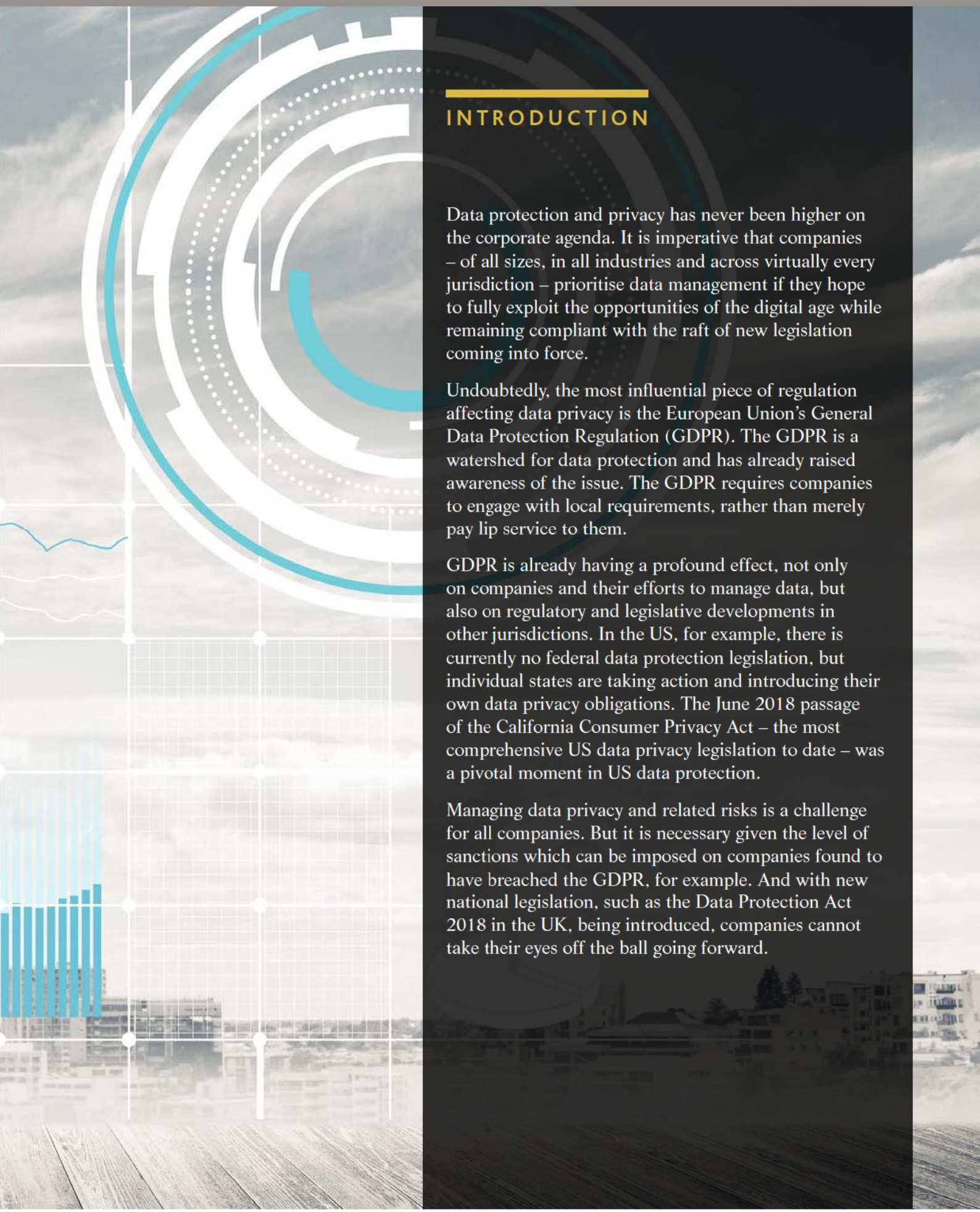
Contents


www.financierworldwide.com

DATA PROTECTION & PRIVACY LAWS

DECEMBER 2018 • ANNUAL REVIEW

Contents



INTRODUCTION

Data protection and privacy has never been higher on the corporate agenda. It is imperative that companies – of all sizes, in all industries and across virtually every jurisdiction – prioritise data management if they hope to fully exploit the opportunities of the digital age while remaining compliant with the raft of new legislation coming into force.

Undoubtedly, the most influential piece of regulation affecting data privacy is the European Union's General Data Protection Regulation (GDPR). The GDPR is a watershed for data protection and has already raised awareness of the issue. The GDPR requires companies to engage with local requirements, rather than merely pay lip service to them.

GDPR is already having a profound effect, not only on companies and their efforts to manage data, but also on regulatory and legislative developments in other jurisdictions. In the US, for example, there is currently no federal data protection legislation, but individual states are taking action and introducing their own data privacy obligations. The June 2018 passage of the California Consumer Privacy Act – the most comprehensive US data privacy legislation to date – was a pivotal moment in US data protection.

Managing data privacy and related risks is a challenge for all companies. But it is necessary given the level of sanctions which can be imposed on companies found to have breached the GDPR, for example. And with new national legislation, such as the Data Protection Act 2018 in the UK, being introduced, companies cannot take their eyes off the ball going forward.

Israel

HAIM RAVIA
Pearl Cohen Zedek Latzer Baratz
Senior 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. He 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. In your experience, do companies in Israel need to do more to fully understand their data privacy and protection duties in the digital age?

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 legislation is the Protection of Privacy Regulations (Data Security), which sets out detailed and prescriptive information security requirements for all companies processing personal data. A few months after the regulations took effect, the Israeli Protection of Privacy Authority, the Israeli privacy regulator, launched a broad, cross-sector inspection campaign at organisations processing personal data in the context of consumer membership clubs, hospitality, medical institutions and clinics, higher education institutions, not-for-profit organisations and others. The second legislation is the General Data Protection Regulation (GDPR), whose extraterritorial reach affects many Israeli companies. In order to prepare for these legislations, companies must meticulously map out their data activities in order to understand what data they process. Our experience shows that in many organisations, data collection and processing is carried out in a non-

systematic manner and through isolated team initiatives. Organisations are then taken by surprise when they learn the true and accurate scope and nature of their processing activities and the personal data they have.

Q. Could you outline the latest legal and regulatory developments affecting corporate storage, handling and transfer of data in Israel?

RAVIA: The Data Security Regulations is a set of rules that took effect in May 2018. The regulations require every organisation that owns, manages or maintains a database containing personal data to implement prescriptive security measures. The main objective of the regulations is to prevent security and breach incidents. These include, for example, physical security measures, access control measures, risk assessments and penetration tests. The regulations classify personal data in four categories – basic, intermediate, high and those held by individuals – with each subject to an escalating set of information security requirements. An amendment to the Israeli Protection of Privacy Law was also proposed, with the aim of enhancing the Israeli privacy regulator's supervisory and enforcement authority. The bill has yet to become law. Additionally, the Israeli government published a memorandum for a Cyber Defence and National Cyber Directorate Bill. The memorandum proposes granting far-reaching powers to the National Cyber Directorate, such as compelling organisations to produce any information or document required to handle cyber attacks and authority to issue instructions to organisations, including instructions to carry out acts on the organisation's computerised material, for the purpose of handling cyber attacks.

Q. In what ways have the authorities increased their monitoring and enforcement activities with respect to data protection and privacy in recent years?

RAVIA: Backed by a new data breach notification requirement, the Israeli privacy regulator is placing considerable attention on data breach incidents. For example, the regulator recently investigated a data breach at an Israeli company in the business of vehicle and fleet location tracking. The data breach was revealed by an anonymous hacker, who exploited a security vulnerability in the company's website, and reported back to the press rather than exploiting the breach for his own malicious benefit. The regulator launched enforcement action against the company and concluded that it had violated the Israeli data security regulations by not providing a timely notice to the regulator about the incident. The regulator has also established a new unit whose focus is broad, sectoral and topical inspections of organisations processing personal data.

Q. What insights can we draw from recent high-profile data breaches? What impact have these situations had on the data protection landscape?

RAVIA: Up until the introduction of the new data breach notification requirement, most breaches have gone unreported. Once the data breach notification requirement took effect, in May 2018, most of the incidents reported publicly have been detected and reported by information security researchers and 'white hat

hackers'. To date, there has been no report of a meaningful 'black hat hacker' or state sponsored data breach incident against commercial companies in Israel. Prior to the data breach notification requirement, the Bank of Jerusalem sustained a notable data breach when hackers infiltrated one of the bank's online trading sites and gained access to the personal data of thousands of consumers, including their names, bank account information, national identification number and date of birth. The privacy regulator's investigation concluded that while the bank had failed to implement appropriate security measures, it had subsequently taken appropriate remediating action to prevent similar attacks in the future. The first post-data breach notification investigated by the privacy regulator was the data breach at the vehicle and fleet location tracking company.

Q. What steps can companies take to mitigate data risks arising from the use of third parties, such as consultants, agents and distributors?

RAVIA: The risk is twofold: a data breach at the third party and the exploitation of the third party as a gateway to data within the company. Recommended steps include proper due diligence checks of the third party and concluding an appropriately protective data protection agreement with the third party. It is always safer practice to not give the third party a copy of the data to keep, but rather grant it narrowly tailored access to the minimal scope of the data it needs to provide the service. If that is not practical, then the third party should be given a copy of the data, in the smallest scope it needs to provide the service, in terms of data volume, time frame and sensitivity. In that case, the third party should be required to keep the data encrypted while in its custody. Procedurally, the commissioning company should bind the third party to its own data security policies and protocols, to inspections and audits, and to effective contractual remedies.

Q. What can companies do to manage internal data privacy risks and threats, such as liabilities arising from lost devices or the actions of rogue employees?

RAVIA: Traditional and long-established information security principles are helpful in safeguarding against these threats. For example, the principle of least privilege requires that each user only be given access to the information and computing resources strictly necessary for his or her role and limiting or completely revoking privileges when the user changes his or her position or leaves the company. Likewise, the principle of data minimisation requires data collection and retention to be limited in the first place to what is necessary in relation to the purposes it is processed for. Data security awareness training, proper HR screening and evaluation and enhanced access controls, such as physical access tokens, all contribute significantly to reducing these risks and are endorsed by the Israeli Data Security Regulations. In fact, compliance with the Data Security Regulations is not only a matter of lawful conduct but can significantly minimise these risks while being up to par with the standard for reasonable security.

"An organisation that tends to mistakenly regard data risk management and regulatory compliance as a task exclusively outsourced to outside counsel and external data security experts is bound to fail."

Q. What essential advice can you offer to companies in Israel on managing data risk and maintaining regulatory compliance going forward?

RAVIA: Companies must realise that managing data risk and maintaining regulatory compliance is a never-ending task that demands the attention of top managers and directors all the way down to low level staff. An organisation that tends to mistakenly regard data risk management and regulatory compliance as a task exclusively outsourced to outside counsel and external data security experts is bound to fail. Organisations must keep abreast of legal and regulatory compliance developments that apply to the sector in which they operate, the jurisdictions in which they do business and the foreign countries whose long-arm laws capture their activities.

www.pearlcohen.com

PEARL COHEN

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

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

DOTAN HAMMER
Senior Associate
+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 represent 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.

www.financierworldwide.com