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

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

Contents

www.financierworldwide.com

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.

United States

JESSICA N. COHEN
Skadden, Arps, Slate, Meagher & Flom LLP
Counsel
+1 (212) 735 2793
jessica.cohen@skadden.com

Jessica Cohen focuses on intellectual property and technology issues in a wide variety of transactions, including licensing and development agreements, outsourcing agreements, service agreements, strategic alliances, and mergers and acquisitions. As part of Skadden's intellectual property and technology group, Ms Cohen counsels clients both large and small on intellectual property protection and ownership issues, and technology implementation and maintenance issues. She also advises clients on general commercial contract issues, including those arising in manufacturing and supply arrangements.

Q. In your experience, do companies in the US need to do more to fully understand their data privacy and protection duties in the digital age?

COHEN: Large mature companies based in the US are generally attuned to their data privacy and protection duties. This is particularly true with respect to multinational companies, many of which used the May 2018 compliance deadline for the European Union's (EU's) General Data Protection Regulation (GDPR) as an opportunity to evaluate their overall data privacy compliance programmes. However, challenges still remain for smaller and less mature companies which may not have the resources or infrastructure to adequately implement comprehensive compliance programmes. In the US, there is a patchwork of data privacy compliance obligations which varies from state to state and from industry to industry, which makes it particularly difficult for companies with fewer resources to identify their compliance responsibilities.

UNITED STATES • JESSICA N. COHEN • SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

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

COHEN: One of the most significant recent developments in the US is the June 2018 passage of the California Consumer Privacy Act (CCPA), which is the broadest and most comprehensive privacy law enacted in the US to date. The CCPA, which comes into force on 1 January 2020, will affect any organisation collecting or storing data about California residents. The intent of the CCPA is to provide California consumers the right to know what personal information is being collected about them, to know whether their personal information is sold or disclosed and to whom, to prohibit the sale of their personal information, to gain access to their personal information and to receive equal service and price, even if they exercise their privacy rights. The CCPA will require many businesses to significantly alter their policies and procedures with respect to the handling of personal information. The California Attorney General has until 2 July 2020 to publish implementing regulations, which will help companies determine how to comply with the CCPA. The Attorney General is prohibited from bringing an enforcement action under the CCPA until six months following the publication of the final regulations or 1 July 2020, whichever is sooner.

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

COHEN: In the absence of US federal data protection legislation, the individual states are taking an increased role in data protection and privacy matters. All 50 states in the US now have some form of data privacy and protection laws. Though such laws initially focused mainly on notification requirements in the event of a data breach involving relatively limited types of personal information, in recent years many states have amended their laws to strengthen data protection for consumers. For example, in 2018, Arizona, Louisiana, Oregon and Virginia all amended their existing data protection laws to expand the definition of personal information. Certain states, such as New York, Colorado and Nebraska, have expanded requirements that explicitly address companies' obligations when providing personal data to third parties.

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

COHEN: In the US, there are frequently data breaches through which hackers gain access to personal information, such as consumer credit card information, social security numbers or other data, but the bigger story has been about data breaches involving unauthorised access to data that is more personal to data subjects, such as their credit history, personal preferences and political views. As a result of such breaches, there is a growing awareness in the US, on the part of both consumers and regulators, regarding the amount and types of data collected from data subjects and the potential harm that unauthorised access to such data can cause. Regulators such as the Federal Trade Commission and the state attorneys general have been aware of this for some time, but thanks to certain recent high-profile breaches, Congress is now showing increased interest in data privacy and protection issues. As a result, the US may be moving closer to federal data privacy and protection legislation.

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

COHEN: First, it is critical that the company have an executed agreement in place with the third party before disclosing any personal data. The agreement should expressly address the third party's scope of permitted use and security obligations with respect to the data. In addition, companies should make sure that third parties have access to the company's data only to the extent necessary to perform the services requested by the company. Depending on the nature of the services and practical considerations, this could mean requiring the third party to work within an area of the company's IT systems, such that the data does not leave the company's premises and the company is able to monitor the third party's use of the data, or requiring the third party to work outside the company's systems with a defined set of data provided by the company, such that the third party's access to the company's data is limited. Finally, it is important to address the handling of personal data at the end of the engagement by requiring the return or destruction of the personal data provided by the company.

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?

COHEN: Companies can implement mandatory data privacy and cyber security training for all employees to make sure they understand the importance of these issues to the health of the company and each employee's role in preventing data privacy violations. The training should emphasise the prompt reporting of lost devices so they can be disabled remotely by the company, and any suspicious activity, such as phishing emails, which employees may be aware of. Companies should also ensure that each employee has access to personal data only to the extent necessary to perform his or her role at the company, which helps minimise the risk of a

"For companies based in the US, managing data risk and maintaining regulatory compliance requires a multifaceted approach to an evolving regulatory landscape."

rogue employee using the data for unauthorised purposes.

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

COHEN: For companies based in the US, managing data risk and maintaining regulatory compliance requires a multifaceted approach to an evolving regulatory landscape. First, companies that collect data from California residents should familiarise themselves with the CCPA, and take steps to bring themselves into compliance by 1 July 2020. Because Californian authorities continue to update and refine certain aspects of the CCPA, companies will need to stay on top of these developments to make sure their compliance plans are revised accordingly. In addition, as other states continue to expand data privacy protections for consumers, companies should take steps to remain current on developments in those states that are relevant to their business. Finally, the extraterritorial application of the GDPR means that companies based in the US that offer services to individuals in the European Economic Area must evaluate whether they are required to comply with the GDPR, if they have not already done so. ■

JESSICA N. COHEN
Counsel
+1 (212) 735 2793
jessica.cohen@skadden.com

United Kingdom

STEVEN JAMES
Brown Rudnick
Partner
+44 (0)20 7851 6103
sjames@brownrudnick.com

Steven James is a partner and solicitor-advocate at Brown Rudnick LLP, and practises in technology, intellectual property and commercial law, with a focus on new technologies and innovation. His experience includes advising clients on contentious and non-contentious intellectual property, data protection and commercial matters in a wide variety of sectors. He also advises on the intellectual property, technology and data protection aspects of a wide range of commercial and corporate transactions. He has been listed as a recommended lawyer in the Legal 500 directory.

Q. In your experience, do companies in the UK need to do more to fully understand their data privacy and protection duties in the digital age?

JAMES: The introduction of the European Union's (EU's) General Data Protection Regulation (GDPR) in May 2018, and the Data Protection Act 2018, which was implemented in the UK shortly afterward, pursuant to the GDPR, appeared to raise the level of awareness of data privacy compliance in the UK to unprecedented levels. Organisations which had perhaps not engaged with local data privacy requirements with the required rigour were suddenly not just papering over the cracks by drafting a privacy policy, but using the exercise to undertake a more systematic review of their data privacy compliance.

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

JAMES: The GDPR has consolidated and reimagined data privacy law in the UK, but the underlying principles have not changed from the previous legislation, the UK Data Protection Act 1998. In a nutshell, organisations need to ensure that they process and collect data fairly, lawfully and transparently. They must ensure that data is collected only for specific and legitimate purposes and that they do not keep excessive amounts of data or keep data for any longer than necessary, that they keep their data accurate and up-to-date and that data is kept secure. Likewise, as under the old law, organisations should not send personal data out of the European Economic Area (EEA) unless safeguarding measures have been taken.

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

JAMES: In the UK, data protection legislation is enforced mostly by the Information Commissioner's Office (ICO). The vast majority of the enforcement action taken by the ICO to date relates to breaches of the old law, which carried a maximum fine of £500,000, so we are still waiting to see what approach the ICO will take to GDPR breaches. However, the implementation of the GDPR appears to have increased the ICO's willingness to issue 'top level' fines under the old law, as two fines of £500,000 were issued in the past two months, to Facebook and Equifax – previously the highest fines were £400,000. The ICO has also issued its first GDPR enforcement notice against a North American company, AggregateIQ, and it will be interesting to see how that is enforced. Another notable factor is that the GDPR has made data subjects much more aware of their rights, so we are anticipating an increased volume of complaints from individuals in the future.

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

JAMES: One of the most important recent cases is *WM Morrison Supermarkets PLC v. Various Claimants*, in which the English Court of Appeal held that Morrisons was vicariously liable for the deliberate actions of its disgruntled employee, even though the company itself had not breached the legislation in any way. This has potentially significant implications for employer liability, and has led to organisations seeking to expand their insurance coverage to include 'inside threats', as well as external breaches. It is also notable that the case was brought by multiple individuals as a civil class action, something which until recently has been historically atypical for data privacy issues in the UK, as enforcement has tended to come from the ICO, but which we expect to see more of in the future. Also, the ICO appears to have an increased appetite for fines for data breaches, even under the old law.

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

JAMES: In practical terms, it makes sense to undertake some background research and due diligence on consultants, agents and distributors. For example, are they familiar with the GDPR and how this affects them, and have they taken appropriate measures, particularly in respect of information security? Do they have any data protection policies in place? It is also essential to put in place effective and robust contractual protections, which may include uncapped indemnities for data breaches, given the size of the potential exposure for the company, and an obligation on the third party to notify the company as soon they become aware of a breach.

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?

JAMES: First and foremost, companies may wish to consider undertaking a comprehensive and ongoing internal training programme, so all employees are aware of their obligations and responsibilities, and are alive to potential risks. In our experience, data breaches are more likely to occur by accident than deliberately, and can often be avoided by anticipating the risks and planning ahead. It is also important to have policies governing data breaches and device use, so that the company is best placed to monitor and mitigate any breach that does occur. Simple

> *"It is important to have policies governing data breaches and device use, so that the company is best placed to monitor and mitigate any breach that does occur."*

technological measures, such as encrypting data and remote wiping of devices, can also be helpful. The *Morrisons* case has also highlighted the importance of insuring against data breaches, as the Court of Appeal made it clear that it expects employers to bear the burden of insuring against the actions of rogue employees.

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

JAMES: The first step is to carry out an internal data audit, so the organisation knows what data it holds, where it came from and how it is used. This information will enable the organisation to review its practices against the GDPR's requirements and prepare a suite of documents, such as privacy notices, retention policies and transfer agreements, which will help it to comply with the regulation. This involves working with internal or external legal counsel, as well as key stakeholders across the organisation, such as IT, human resources, group heads and risk management, to identify potential risks and weaknesses, and to develop mitigation strategies. Depending on the nature and sensitivity of the data involved, it may also be helpful to involve external IT consultants such as security experts and penetration testers.

STEVEN JAMES
Partner
+44 (0)20 7851 6103
sjames@brownrudnick.com

MARK LUBBOCK
Partner
+44 (0)20 7851 6062
mlubbock@brownrudnick.com

RUTH ARKLEY
Associate
+44 (0)20 7 851 6156
rarkley@brownrudnick.com

Germany

DR JOCHEN LEHMANN GÖRG
Partner
+49 221 33660 244
jlehmann@goerg.de

Dr Jochen Lehmann has been a partner at GÖRG since 2007 and specialises in IT matters, with a particular focus on data protection and data security. He has built his expertise in this particular field of law since he began working for GÖRG 18 years ago. Dr Lehmann is a regular speaker on the subject of data secrecy and data protection in various contexts, such as data secrecy and directors' liability or data secrecy and insurance.

Q. In your experience, do companies in Germany need to do more to fully understand their data privacy and protection duties in the digital age?

LEHMANN: On the whole, companies do need to do more. There are, of course, those companies that fully understand the opportunities presented by the digital age, but there are also risks and so they act accordingly. But recent surveys have shown that a lot of companies, even in areas such as healthcare, are neither prepared to adapt their business activities nor, in particular, their security provisions. This is all the more surprising as it is not only essential for any company to be compliant – given the heavy fines available to the regulators – but also rather short-sighted because customers, consumers in particular, often show less patience with companies that are careless with personal data. Any company which is not compliant with the GDPR should, therefore, increase its efforts.

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

LEHMANN: In Germany, the most important development over the last year was the implementation of the European Union's (EU's) General Data Protection Regulation (GDPR). The GDPR overhauled the data protection landscape by ensuring that both data protection and data security now receive the attention they deserve, even if compliance with the new regulation is still not achieved by a lot of companies and despite the fact that the German regulators have not yet imposed significant fines. The implementation of the GDPR aside, no other major developments have taken place of late, most likely because of the time taken to form the new government.

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

LEHMANN: Currently, German regulators are more or less fully occupied with work relating to the implementation of the GDPR, in particular with answering thousands of questions from data controllers. However, German regulators have recruited new personnel and have already announced that they will be putting greater emphasis on monitoring activities such as sending questionnaires to a large number of enterprises. Regulators have also announced that they will start exercising their power to impose fines on non-compliant enterprises soon. During the course of 2019 the period of grace for companies not willing to comply or being too slow to achieve compliance may end.

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

LEHMANN: The main insight we can draw from recent breaches is that every enterprise is vulnerable. Therefore, companies must increase their security provisions, knowing that one day a data breach might happen. However, that breach might cause much less damage if the company is prepared. An essential part of that preparation

is the location of resources that are able to assist when disaster strikes, such as forensic experts, public relation experts and, of course, technical means that allow a timely reset and restart of the IT. Also, the board of directors should, at least in theory, have a strategy for coping with such an incident, not least because it is mandatory under the GDPR. Reports of increased data breaches have boosted the sale of cyber insurance. And, finally, the German government, namely the Ministry for the Interior, has announced that new proposals will soon be made regarding cyber security, but nothing concrete has yet appeared.

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

LEHMANN: Companies should try to reduce third-party access to their IT to the absolute minimum and, if possible, provide third parties with computers that are monitored by themselves instead of offering third parties full access via their own devices. Each access should be logged and log-files should be safely stored. Another option is to concentrate relevant information in a single point of access, such as a SharePoint, where information can be accessed but further access to IT systems is prohibited.

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?

LEHMANN: Companies must have a detailed reporting scheme for the loss of devices and similar incidents. There has to be, ideally, one point of contact for all incidents concerning the loss of mobile devices. And every company needs detailed internal sets of rules governing how such an incident should be notified internally and what should happen afterwards. That set of rules should be made available throughout the company so that when the loss happens, no questions need to be asked. Also, mobile devices should have hard disk-encryption. However, the loss of devices is just one problem. The far greater danger results from employees who, for whatever reason, are either too careless with data or even steal data. Employees and their activities should therefore be monitored as closely as legally permitted in order to identify suspicious patterns of data processing and to detect any possible data breaches.

"Companies should try to reduce third-party access to their IT to the absolute minimum and, if possible, provide third parties with computers that are monitored by themselves instead of offering third parties full access via their own devices."

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

LEHMANN: The essential advice is that companies should have a comprehensive security scheme in place. Without a strategy to enhance data security, all efforts are bound to fail or fall short of expectations for several reasons: the staff will not accept half-hearted efforts, the work-flows will not fit in and, worst of all, without a clear objective success cannot be measured. If activities and procedures have to be adapted to fulfil the objectives of data protection and a data security scheme, as burdensome as this may seem, such changes must be made. This effort will, in all likelihood, pay off because these activities will be more streamlined and more effective afterwards. Moreover, this reduces the risk of directors being held personally liable for any loss of data and the ensuing loss of business.

www.goerg.de

GÖRG

GÖRG is one of Germany's leading business law firms. As an independent law firm with 290 lawyers and tax advisers at five offices in Berlin, Cologne, Frankfurt am Main, Hamburg and Munich, GÖRG advises on the core areas of business law. GÖRG has a leading reputation in insolvency law and restructuring projects and is top ranked in all core areas of business law, including corporate, real estate and procurement law. Nationwide, the firm ranks among the top 20 law firms.

DR JOCHEN LEHMANN
Partner
+49 221 33660 244
jlehmann@goerg.de

Italy

FRANCESCO DE BIASI
Cleary Gottlieb Steen & Hamilton LLP
Counsel
+39 06 6952 2254
fdebiasi@cgsh.com

Francesco De Biasi's practice focuses on private enforcement and internal investigations of corporate wrongdoing with a focus on the requirements of Italian Legislative Decree No. 231/2001, as well as on corporate, civil, labour law and data protection matters related to white-collar crimes. Mr De Biasi also has extensive experience in international litigation, with an emphasis on corporate, commercial and financial matters. He has been involved in many private enforcement cases concerning Italian subsidiaries of multinational groups, including the civil and corporate litigation arising therefrom. He is contract professor of internet law at the Pontificia Università Lateranense in Rome.

Q. In your experience, do companies in Italy need to do more to fully understand their data privacy and protection duties in the digital age?

DE BIASI: We have noticed a significant increase in company awareness of privacy and data protection obligations, not only in light of the high level of fines that the European General Data Protection Regulation (GDPR) currently imposes on them, but also in light of the potential reputational risks that non-compliance with privacy and data protection laws may entail. We have noticed that, as a consequence, more companies have adopted a preventive and group-level approach to privacy and data protection matters in general, and, in particular, to comply with the GDPR. However, many companies are still grappling with the practical implications that their new data privacy and data protection duties entail; in other words, rather than an issue of awareness, we believe it is more an issue of how to translate such awareness into practice. Even more so than in the past, complying with data protection laws in general, and with the GDPR in particular, goes beyond mere paperwork and requires a more substantial approach.

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

DE BIASI: The GDPR became directly applicable in Italy, as in all EU Member States, on 25 May 2018. Furthermore, the Italian Data Protection Code was amended by Legislative Decree No. 101 of 10 August 2018, which entered into force on 19 September 2018. The purpose of the Legislative Decree was, among other things, to repeal those national provisions deemed incompatible with the GDPR and insert additional provisions based on clauses contained in the GDPR that allow EU Member States to enact laws on certain aspects, such as the provision on limiting data subjects' rights to safeguard, for example, national security, or the prevention, investigation, detection or prosecution of criminal offences. In addition, the Italian Data Protection Authority (IDPA) is currently engaged in an extensive review of the authorisations and general provisions it has issued and the codes of conduct it has adopted to date. In parallel, the IDPA has started to take advantage of certain new powers granted by the GDPR. Most notably, the IDPA has issued a list of the kind of data processing operations which are subject to the requirement of a data protection impact assessment, pursuant to Article 35(1) of the GDPR. Consequently, the post-GDPR Italian data protection legislative framework is not necessarily final.

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

DE BIASI: According to the IDPA's Report on Activities 2017, the IDPA carried out 275 investigations of both the private and public sectors in 2017 and found 589 infringements and imposed fines of €3,776,694 – an increase of around 15 percent on 2016. In addition to its proactive investigations, we have noticed that in recent years individuals have increasingly availed themselves of the mechanisms available to raise complaints to the IDPA and thus possibly trigger IDPA investigations into those companies involved. According to the 2017 Report, the IDPA provided its feedback on 5819 complaints, an increase of 1186 on 2016. Turning to the sectors where the IDPA appears to be more active, the lawfulness of data

processing activities for marketing purposes, including social spamming and data processing in the employment context, including potential monitoring of employees by means of company devices, appear to be almost always on the IDPA's radar.

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

DE BIASI: Data breaches give rise to reputational damage, which can be even more burdensome for companies than the administrative fines that could be levied after the data breach itself. Indeed, reputation is intertwined with trust and, once damaged, takes time to be restored. To minimise potential reputational damage, companies should put in place measures and procedures, among other things, that enable them not to underestimate events or anomalies that could give rise to a data breach, and to promptly notify the competent Data Protection Authorities, as well as the data subjects, of the data breach.

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

DE BIASI: We recommend performing preliminary due diligence of third parties to establish whether the third parties comply with applicable data protection legislation, including the security measures they adopt. As a minimum, they could be asked to complete a questionnaire covering certain key aspects of their operations, such as what technical and organisational security measures are in place and whether personal data is stored in the European Economic Area (EEA) and, if so, whether a transfer outside the EEA is envisaged. Furthermore, as the GDPR makes companies and their vendors jointly and severally liable for non-compliance, it is important for companies to seek contractual protection in relation to damages for which only one party is responsible. Lastly, companies may be dependent on processors with reference to information to be provided, for instance, to supervisory authorities, and data subjects, under the circumstances, in relation to data breach notifications. This circumstance should be properly taken into account when drafting data processing agreements with third parties by providing, for example, specific timing for the processors to provide the necessary information, rather than relying on the 'without undue delay' standard.

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?

DE BIASI: Awareness of how personal data flows to and from the company, including within a group of companies, if applicable, and who has access to it are key to efficient management of any personal data-related risk. Secondly, companies should clearly inform their employees of permitted uses of company devices and networks by adopting, and publicising, internal policies. Thirdly, companies should properly and regularly train employees handling personal data, with a view to fostering a company-wide culture of data protection and privacy.

"Despite the inevitable regulatory changes that companies will have to deal with in the future, the basic principles of data processing are likely to remain substantially unchanged."

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

DE BIASI: Despite the inevitable regulatory changes that companies will have to deal with in the future, the basic principles of data processing are likely to remain substantially unchanged. For example, lawfulness, fairness and transparency of data processing, processing only the personal data necessary in relation to the purposes for which it was collected, storing personal data only for the time necessary in relation to the purposes for which it is processed and, above all, accountability, which requires companies to comply with data protection laws and to be able to demonstrate that they do so, as well as following the principles of privacy by design and by default. Complying with the principles of data processing will allow companies to maintain regulatory compliance smoothly and in a cost-efficient manner going forward.

www.clearygottlieb.com

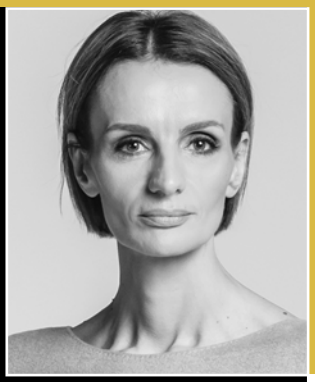
CLEARY GOTTLIEB

Cleary Gottlieb Steen & Hamilton LLP has been a leader in the legal profession for more than 70 years. With a network of specialists in 16 offices on four continents, it regularly advises clients in diverse industries on the privacy, data protection and cyber security challenges impacting their businesses. Its privacy and cyber security task force works collaboratively across practice areas and jurisdictions to advise domestic and multinational clients not only on legal obligations and liabilities, but also on anticipated changes in laws and enforcement practices, strategies for managing compliance and risks, and minimising the costs and efforts of compliance.

FRANCESCO DE BIASI
Counsel
+39 06 6952 2254
fdebiasi@cgsh.com

ANDREA MANTOVANI
Associate
+39 06 6952 2804
amantovani@cgsh.com

EVA REGGIANI
Associate
+39 02 7260 8676
ereggiani@cgsh.com



Serbia

LJILJANA URZIKIC STANKOVIC
Stankovic & Partners
Partner
+381 64 169 53 76
ljiljana.urzikic@nstlaw.rs

Ljiljana Urzikic Stankovic is a partner at Stankovic & Partners. She has extensive experience providing advisory services to parties in Serbia on matters of data protection and intellectual property (IP) law. As an expert in this field, Ms Urzikic Stankovic focuses on all matters related to the processing of personal data and the protection of IP rights, including trademarks, design rights and patents, as well as handling cyber crime and anti-piracy issues. Her broader commercial expertise also includes labour and employment law, and banking and finance with a particular emphasis on project finance and securitisation.

Q. In your experience, do companies in Serbia need to do more to fully understand their data privacy and protection duties in the digital age?

URZIKIC STANKOVIC: In the last few years, companies in Serbia have become more aware and have a better understanding of the concept of privacy and personal data protection. Crucially, the new Law on Data Protection has recently been adopted. Prior to that, the previous law governing data protection was introduced in 2008, and for a long time, data privacy and protection were relatively new and unknown concepts for many Serbian companies. The most important changes in this field have been felt as a result of the enforcement of the European Union's (EU's) General Data Protection Regulation (GDPR). Though the GDPR applies only to those companies which process the data of EU citizens or have businesses within the EU, the implementation of the GDPR has led to a better understanding of the significance of data protection and privacy obligations of companies in Serbia.

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

URZIKIC STANKOVIC: Serbia is increasingly dedicated to digitalisation. The introduction of e-government, and the adoption of new regulations in this field, have reflected the new significance placed on data protection in Serbia and these measures have led to the replacement of traditional solutions for corporate storage, handling and transfer of data with new solutions. This primarily refers to the new Law on Personal Data Protection, the Law on Information Safety, the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Transactions (E-Business Law) and other laws.

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

URZIKIC STANKOVIC: In Serbia, the Commissioner for Information of Public Importance and Personal Data Protection, an independent state body, has been introduced with the aims of protecting personal data. The scope of the Commissioner's work is defined by the law. So far, the legal framework governing personal data protection has not been completely or fully defined. The consequence of this is the violation of the right to personal data protection and the right to privacy. From the report of the Commissioner for Personal Data Protection, based on available records of a number of cases, there were numerous successful interventions in 2018, but there are still many criminal complaints submitted to the Commissioner regarding the unauthorised collection of personal data which remain unsolved. That is why this process should be more efficient, something which is expected after the implementation of the new Law on Personal Data Protection, which has been adopted recently and which envisages the following novelties: the chance to submit complaints to the Commissioner and the chance for individuals to directly address the court with a lawsuit.

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

URZIKIC STANKOVIC: Several incidents of data 'leaking' in big companies have certainly damaged the illusion of data safety and privacy in the cyber space, and have had a significant impact on the understanding of privacy and personal data protection. Internet users are now more interested in the protection of their privacy and are acting more responsibly toward their data. Many companies are also searching for solutions which would protect that data.

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

URZIKIC STANKOVIC: In the initial phase, before the collection of data, it is necessary for companies to correctly determine the scope and type of personal data to be collected, and then establish the rules for further use of that data. This will significantly reduce risks arising from the use of personal data by third parties. For legal entities, it is often more economically efficient to establish rules for the use of data, since the resources available to users are adapted to the scope and type of data to be collected. Internal procedures for use of personal data may define which data is collected. These procedures must also consider the reasons for collection, defining which individuals have the right to access personal data, regulate the process for transfer of data to third parties, and so on.

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?

URZIKIC STANKOVIC: With the increasing digitalisation of business, data is becoming a key resource in all industries. The equipment used to transfer personal data has become a key channel for company networks. While guaranteeing the physical safety of equipment can be difficult, there are still ways to protect the data stored on them, by encrypting computers and disks, as well as configuring equipment in order to control and protect passwords, manage remote deletion of personal data and locate lost equipment. In addition, employees should be informed about data management and maintenance through clearly defined rules on data management and storage. One of the most significant steps companies can take is to test whether they are ready for an incident. A test should be carried out at least once, and the reaction times and efficiency of all team members should be measured.

"Personal data protection requires practical knowledge of suitable legal mechanisms, as well as relevant experience, as this legal area is constantly changing and growing."

Sometimes, such incidents can be prevented by educating employees, which is a step often overlooked by companies.

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

URZIKIC STANKOVIC: Personal data protection requires practical knowledge of suitable legal mechanisms, as well as relevant experience, as this legal area is constantly changing and growing. In an era where companies are amassing personal data in greater volumes, one of the main ways in which firms can differentiate themselves is through their ability to secure privacy for their employees and clients. Personal data processors and controllers should estimate the impact of processing personal data protection. Companies should publish their internal policies and procedures governing the management of personal data. They should also appoint individuals who will be responsible for personal data processing and who will control, suggest and undertake measures related to personal data protection. Finally, companies must understand their role in respect of the personal data they process, and must, consequently, determine their flow within the company and outside of it, and thus prevent or discover every possible abuse of personal data in a timely fashion.

www.nstlaw.rs

nstlaw/Stankovic & Partners

Established in 2010, Stankovic & Partners is a full service firm located in Belgrade, Serbia, with a team of experts who advise multinational corporations and Serbian and Montenegrin companies, often acting in cooperation with well-known international law firms. The firm has received a number of national and international accolades, including recommendations by *Chambers & Partners' Europe* and *Global Guides, The Legal 500, EMEA* and *IFLR*.

LJILJANA URZIKIC STANKOVIC
Partner
+381 64 169 53 76
ljiljana.urzikic@nstlaw.rs

Romania

MARTA POPA
Voicu & Filipescu
Senior Partner
+40 21 314 02 00
marta.popa@vf.ro

Marta Popa has wide experience in various practice areas under Romanian law, including corporate consultancy, mergers and acquisitions, data protection matters, as well as project finance, public procurement, energy and employment law. She is a very experienced lawyer on data protection, advising international and local companies on all aspects of data protection law and practice, including GDPR end-to-end implementation and compliance projects, as well as GDPR audits. In the employment context, she was involved in compliance assessments regarding the use of employees' private data and advised on complex issues regarding the monitoring of their work activity.

Q. In your experience, do companies in Romania need to do more to fully understand their data privacy and protection duties in the digital age?

POPA: A first step toward General Data Protection Regulation (GDPR) compliance is a proper analysis of the internal business operations of a company, drawing up adequate and real data flows, followed by a proper GDPR gap analysis. Many Romanian companies, especially major but also small companies whose activity is data-sensitive, have made progress in complying with the GDPR which is, in part, due to Romania having highly skilled IT and security specialists who are involved in the process. There is still room for improvement until a significant number of local companies understand how the GDPR is impacting their business, which is a matter of management being aware of and educated about the impact and risks of digitalisation. For example, organisations are taking more of their data and applications to the cloud, thus increasing the risk of a cyber security incident, but are unaware of the related risks. However, the GDPR compliance rate remains low in Romania, with only 30 to 35 percent of companies achieving a satisfactory level of compliance. Given the benefit of having a skilled IT force, we believe that in the

years to come, organisations in Romania will become more and more educated and aware of the consequences of digitalisation.

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

POPA: As of 31 July 2018, Romania adopted national measures for implementation of the GDPR through Law no. 190/2018. Law no. 190 establishes special rules on the processing of certain categories of personal data which take into account: genetic data, biometric data or health data, national identification number, personal data processing in the context of labour relations, personal data, and special categories of data in the context of performing a task that is of public interest. More specifically, with regard to the storage of data, Law no. 190 provides for special data processing conditions consisting of national identifiers, such as a personal identification number, identity card number and series, passport number, driving licence number or social health insurance number.

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

POPA: The areas where most complaints were made, and increased monitoring and enforcement actions taken, related to processing of personal data in the context of credit checks at the credit bureau and video monitoring of electronic communications. However, such actions were insufficiently publicised in the media. In addition, the insignificant level of penalties applied – a maximum of €2000 – added to the lack of impact on companies. Generally speaking, while the data protection authority's profile in Romania was low until the GDPR's entry into force – except for 2017, when companies' preoccupation with conforming to the GDPR started to show in an increased number of data-related claims and data breach notifications 2018 has seen an increase in the profile and activity of the Romanian regulator. During 2018, Romania has adopted a series of national measures for implementing the GDPR, providing clarification of certain provisions, or derogations and exceptions where allowed under the GDPR.

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

POPA: Recent data breaches seem to have had the effect of 'lessons learned' for many companies. No organisation wants to find itself in the tough position of disclosing a data breach and protection of personal data seems to be paramount for companies which are processing this type of data. The consequences can be both immediate and long term, for the company as well as for its customers. Companies should learn that data breaches may damage the company's value and reputation, and lead to potential regulatory fines, lawsuits and victim compensation. While it seems that individuals are more careful than ever about how their data is used by controllers, controllers themselves seem to be more aware of the risks of the increasingly advanced set of tools and techniques used to perpetrate breaches. We have seen an increased interest in Romanian companies compiling an adequate set of technical and organisational security measures to protect individuals' data and a willingness to provide these to contractual partners when they conclude contracts involving data processing.

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

POPA: When using external service providers, companies should put in place a set of GDPR compliance audit control rules and procedures to check their compliance. The audit should cover their data protection policies of their providers, employee confidentiality, management quality systems certifications and general technical and organisational measures.

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?

POPA: The first measure would be to raise awareness of the existing business processes, data flows, vulnerabilities and associated risks affecting the rights and freedoms of individuals. Secondly, depending on the asset type, identified vulnerability and potential risk, different measures can be taken, such as changes to business processes, switching processors, encrypting for data in transit and at rest, asset and device management, and data classification and protection.

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

POPA: Companies should not rely on other companies' experience or on policies or measures available from public sources. There is no ready-made or 'one-size-fits-all' solution. The best approach towards compliance with GDPR requirements is to take on board experienced GDPR specialists who can provide end-to-end conformance advice from a 360-degree perspective. In our view, the consultant team should include specialised lawyers, and specialised IT and cyber security specialists. Additionally, the compliance burden should not be placed on external consultants, but should

"The best approach towards compliance with GDPR requirements is to take on board experienced GDPR specialists who can provide end-to-end conformance advice from a 360-degree perspective."

actively involve staff members. As part of the initial compliance process, a company should implement training to ensure its internal team has been made aware of GDPR requirements. Going forward, once a satisfactory degree of compliance has been achieved with the help of GDPR specialists, a company must be aware that GDPR compliance is a continuous process. Among other measures, companies must refresh knowledge of GDPR requirements by providing periodic training. Last, but not least, companies should engage with a good data protection officer (DPO) who can be consulted whenever a new business process in which personal data are used or new technologies are involved is initiated. ■

www.vf.ro

VOICU FILIPESCU
Attorneys at Law

Since its establishment in 2001, Voicu & Filipescu has been one of the top Romanian law firms in terms of turnover, market position and reputation. Today the Voicu & Filipescu group include the law firm, a dedicated tax and accounting company and a specialised insolvency practice. In the data protection field, the firm offers expert advice to clients acting in various industries covering the full range of issues including GDPR compliance, data protection audits and trainings, data processing and transfer agreements, the preparation of PIA and DPIA, processing and the transfer of employee personal data, among others.

MARTA POPA
Senior Partner
+40 21 314 02 00
marta.popa@vf.ro

DANIEL VOICU
Managing Partner
+40 21 314 02 00
daniel.voicu@vf.ro

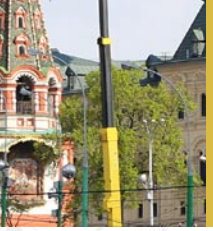
Russian Federation

SERGEY MEDVEDEV
Gorodissky & Partners
Senior Lawyer
+7 495 937 6116
medvedevs@gorodissky.ru

Sergey Medvedev is a senior lawyer in Gorodissky & Partners' Moscow office, where he works in the intellectual property (IP) and technology, media and telecommunications (TMT) group. With more than 10 years of professional legal experience, he advises clients on all aspects of Russian law associated with IP and TMT, internet and e-commerce, data protection and privacy, software development and protection, licensing and outsourcing, franchising and distribution, media and advertising, dispute resolution and anti-counterfeiting. He is a frequent speaker at different international law conferences and an author of many publications devoted to various IP and TMT issues, including data privacy.

Q. In your experience, do companies in the Russian Federation need to do more to fully understand their data privacy and protection duties in the digital age?

MEDVEDEV: Data privacy and protection has become one of the most discussed topics in the information technology (IT) sector in recent years. In the digital age, amid evolving data privacy laws, companies, including those operating in Russia, as well as foreign investors, should carefully assess their data protection strategies and achieve data privacy compliance to mitigate the associated risks. However, not all of them are fully aware of their rights and obligations in this particular area, especially their confidentiality duties, required security measures, data transfer rules and the 'localisation' requirement, when processing personal data online or offline. Indeed, this might be a big challenge for them following the imposition of tougher sanctions for data breaches on a local and global level. More specifically, I am talking about the recently introduced new local administrative fines for various privacy violations and the implementation of the General Data Protection Regulation (GDPR).



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

MEDVEDEV: Of course, companies that are data operators should have an understanding of the major legal and regulatory requirements affecting collection, storage and transfer of personal data in Russia. First, when collecting personal data, the data operator must provide the data subject with certain required information, including but not limited to, the legal grounds and purposes of data processing, methods and duration of data processing, as well as information on cross-border data transfer, if required. If the provision of personal data is mandatory under the law, the data operator is obliged to explain to the data subject the legal consequences of refusing to provide such personal data. In those cases where personal data is collected through the internet, the data operator is obliged to ensure that the recording, systematisation, accumulation, storage, clarification and extraction of personal data related to citizens of the Russian Federation is made with the use of databases located within the Russian Federation. In other words, the 'localisation' requirement must be met under the national data protection law. Retention of personal data must be done in a form which allows the data subject to be defined for as long as the purposes of data processing are effective or necessary, unless the specific term of storage of personal data is set forth by the law, or by the agreement to which the data subject is a valid party, beneficiary or guarantor. Personal data must be destroyed or anonymised as soon as the objectives of the data processing have been achieved, or in the event that the achievement of such purposes is no longer effective or necessary, unless otherwise is provided by the law. The transfer of personal data outside of Russia is regulated under Article 12 of the Personal Data Act. In the event of a cross-border data transfer, the data operator must ensure, before such a transfer is made, that the rights and interests of the respective data subject are fully protected in an 'adequate manner' in the corresponding foreign country. Cross-border data transfer to countries that do not provide a level of 'adequate protection' is permitted if the written consent of the respective data subject has been received, or it is made for the performance of the contract to which the data subject is a party to.

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

MEDVEDEV: It is very important to note that local data privacy laws have been heavily enforced in recent years, and the Russian Data Protection Authority is quite active in terms of monitoring data protection compliance. There have been a growing number of data breach cases lately, and the national court practice devoted to data privacy enforcement is developing constantly in Russia. From 1 July 2017, the administrative sanctions for different privacy violations were increased substantially. For example, data processing, which is not in line with legal requirements for the volume of data provided in the written consent of the data subject, may result in a fine of RUR 75,000. Also, in the case of illegal data processing on the web, access to the infringing website may be blocked in Russia via court decision. Criminal prosecution and imprisonment is available for certain specific categories of privacy violations.

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

MEDVEDEV: Recently, the social network 'LinkedIn' has been blocked in Russia for not meeting the 'localisation' requirement. Also, in *Telegram*, the Russian court fined the instant messaging service RUR 800,000 for failing to provide the Federal Security Service (FSS) with the decoding keys, as prescribed by Article 10.1 (4.1) of the Russian Data Protection Act. On 22 October 2018, Telegram's appeal was rejected and the administrative fine was enforced. The law requires all messaging services to ensure the confidentiality of their users' communications. In this case, FSS, although entitled to see such communications by law, was refused access by *Telegram*, which argued that it lacked control over the encoding and decoding processes. The Telegram case shows that if the relevant technology of the messenger does not allow state authorities to gain access to the decoded information, including certain categories of personal data, this may be deemed a data breach.

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

MEDVEDEV: Third-party processors, including consultants and agents, are basically subject to the same legal requirements as data operators, and they must comply with established data processing rules. Usually, such third parties will be acting under specific data processing agreements, and data operators will be liable for all acts or omissions of processors in front of data subjects, while respective processors must take responsibility before data operators. Importantly, data subjects must consent to the transfer of their personal data to third-party processors.

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?

MEDVEDEV: Internal data privacy risks and threats, such as those arising from lost devices and data leaks, can be mitigated through the implementation of necessary and sufficient

"Third-party processors, including consultants and agents, are basically subject to the same legal requirements as data operators, and they must comply with established data processing rules."

security measures prescribed by local laws, regulations and standards. In other words, certain legal, technical and organisational steps have to be undertaken in terms of overall data processing management and compliance. When processing the personal data of employees, it is also very important to have a clear picture of general data protection requirements set forth by the national labour legislation, in addition to requirements provided by the Russian Data Protection Act and the Russian Personal Data Act.

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

MEDVEDEV: It is essential to manage data risks and maintain regulatory compliance properly. For these particular purposes, the appointment of data protection officer (DPO), the adoption of a data protection policy, and other required documents, as well as the implementation of appropriate security measures, will be the first key things to do. Allocating functions and responsibilities between competent employees is also necessary. Parties should conduct periodic data privacy audits and ensure ongoing data security controls are in place and that the company is compliant with national data protection requirements. ■

www.gorodissky.com

GORODISSKY

A home-grown and full-service Russian IP boutique, Gorodissky & Partners, with its headquarters in Moscow, 12 branch offices in Russia and one in Ukraine, is a leading firm in every aspect of the protection, disposal and enforcement of IP and IT rights. Though the firm's main jurisdictions are Russia and Ukraine, thanks to its trusted network, Gorodissky & Partners represent national and international clients around Eurasia and CIS countries. It is the largest IP practice in Russia and among the top 10 biggest IP law firms in Europe. The firm was originally founded by patent/trademark attorneys and lawyers in 1959.

SERGEY MEDVEDEV
Senior Lawyer
+7 495 937 6116
medvedevs@gorodissky.ru

Pakistan

SAIFULLAH KHAN
S.U.Khan Associates
Managing Partner
+92 51 234 4740
saifullah.khan@sukhan.com.pk

Saifullah Khan is an international trade lawyer, with 20 years' experience in international trade policy and law advisory, serving foreign and Pakistani clients. He has also advised the Pakistani government in the amendment of trade defence laws and rules. Furthermore, Mr Khan has an extensive global advisory portfolio in international trade management system, international trade agreements and para-tariff and non-tariff barriers issues. Mr Khan has also gained experience in policy and regulatory framework regarding e-commerce. He is a Fellow Member of the Institute of Cost & Management Accountants (ICMAP) and the Pakistan Institute of Public Finance Accountants (PIPFA).

Q. In your experience, do companies in Pakistan need to do more to fully understand their data privacy and protection duties in the digital age?

KHAN: Pakistan is in the process of introducing data protection legislation similar to the EU's General Data Protection Regulation (GDPR). GDPR, due to its territorial scope, is applicable to web shops established in Pakistan. Local and global incumbent obligations on companies in Pakistan certainly require them to do more to fully understand their data privacy and protection duties. In particular, local legislation, when enforced, would require companies to take steps to become fully compliant with legal obligations. The proposed legislation aims to put extensive obligations upon companies – in their capacity as data controller or data processor – so it is the right time for companies to study best international practice in order to introduce new processes.

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

KHAN: In June 2018, the Ministry of Information Technology prepared a draft of the proposed Personal Data Protection Law. The draft is under consultation and will be tabled before the National Assembly of Pakistan. In 2016, Pakistan introduced the Prevention of Electronic Crimes Act, 2016 which recognises the unauthorised access and processing of data as being a criminal offence under the Criminal Procedure Code, 1898, which stipulates imprisonment and financial penalties as punishment. The Payment Systems and Electronic Funds Transfers Act, 2007 also provides for the secrecy of financial institutions' customer information and violation is punishable with imprisonment or financial fine, or both. The Electronic Transactions Ordinance, 2002 – introduced in line with the UNCITRAL Model Law on e-Commerce 1996 – also designates unauthorised access to information as an offence and is similarly punishable.

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

KHAN: Authorities are relying on biometric identification and verification systems. Most G2C and B2C transactions are authenticated by means of thumb impressions saved by the national database authority, for example subscribing for cellular phone connection, opening a bank account, ATM cards, passports and motor vehicle registration. Even older mobile subscribers and bank account holders are required to visit these companies and financial institutions to record and retrieve their thumb impressions from the national database authority. In addition, the Pakistan Telecommunication Authority monitors inappropriate and misleading websites and social platforms in order to detect violations of the Prevention of Electronic Crimes Act, 2016, and banks and financial institutions under the direction of the State Bank of Pakistan have extended Know Your Customer (KYC) parameters in order to combat any possible data breach.

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

KHAN: Recently, Pakistani bank data was cyber attacked, with customers receiving notification about money transfers from their account. Following various abnormal international transactions and complaints from customers, the affected bank immediately reacted and shut down its system to stop further transactions. This timely action helped keep losses to Rs 2.6m as opposed to Rs 5 to 6m. Currently, the State Bank of Pakistan and relevant agencies are investigating the incident. Pakistan's Prevention of Electronic Crime Act, 2016 has already brought unauthorised interference with an information system and transmission of data as a criminal offence. Moreover, the State Bank of Pakistan has directed all banks to take steps to identify and counter any cyber threat to their IT systems in coordination with international payment schemes.

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

KHAN: Companies can take various steps to mitigate data risks that may arise due to engagement with third parties. Before entering into any relationship, companies should carry out a privacy and data protection risk assessment of the third party. Performing appropriate due diligence when selecting third parties that will have access to company data, systems and facilities is another means to mitigate risk. Third parties must be subjected to ongoing oversight and this should be adjusted based on the type and volume of data handled. Companies can further reduce risk and liability by ensuring they have contractually protected themselves. In their agreements with third parties, companies should ensure that third parties comply with certain data security and privacy practices, and that companies can audit third-party practices.

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?

KHAN: Companies should develop specific policies and procedures to handle proprietary or sensitive information. Employees should be required to sign an acknowledgement indicating they have read the policies and understand their responsibilities. Employees should be offered appropriate and specific training about these responsibilities and the consequences of unintentional exposure or unauthorised access to protected information. Companies should also take steps to ensure that only the minimum required access to data is given to employees. Companies must communicate and apply consistent sanctions for information privacy or security violations. Employee activities should be regularly monitored. This ensures appropriate access and can detect unusual activity. Adequate oversight or governance of information security programmes also helps to evaluate the causes of security or privacy incidents, apply consistent sanctions, monitor training activities, and allocate resources to mitigate and remediate prohibited disclosures.

"Performing appropriate due diligence when selecting third parties that will have access to company data, systems and facilities is another means to mitigate risk."

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

KHAN: Companies need to determine exactly what data they hold. Companies then need to establish how this data was obtained and whether consent to hold this data was also obtained. Companies need to determine their legal basis for processing personal data. Companies should be able to recognise and respond to requests from data subjects, for example the right to object or the right to be forgotten. All processes must be clearly documented and become part of their business processes. Moreover, employees should be suitably trained to respond to vulnerabilities and data breaches. In addition, companies need to review their existing business processes with respect to data protection, privacy policies and privacy statements, in order to conform to international best practice. A compliance checklist is useful in this regard, as is appointing someone to be in charge of data protection obligations.

www.sukhan.com.pk

S.U.Khan Associates
Corporate & Legal Consultants

S.U.Khan Associates was established with the aim of providing a distinctive range of services to its clients in Pakistan, as well as globally. The firm sees its purpose as turning knowledge into value in order to provide its prestigious clients with a consistent set of multidisciplinary services, based on profound industry knowledge. With soaring aspirations and the zeal to succeed, the firm endeavours to be a recognised and reputed global professional service provider.

SAIFULLAH KHAN
Managing Partner
+92 51 234 4740
saifullah.khan@sukhan.com.pk

SAEED HASAN KHAN
Partner
+92 345 513 9603
saeed.hasan@sukhan.com.pk

India

ANIRUDH RASTOGI
Ikigai Law
Founder
+91 98991 44333
anirudh@ikigailaw.com

Anirudh Rastogi is the founder of Ikigai Law and specialises in advising technology businesses and investors on general corporate, regulatory and policy issues. An alumnus of the Harvard Law School, he was named achiever of the year 2017 by Business World magazine for his work with cutting-edge tech ventures, including advising on a lunar mission and India's early crypto-exchanges. He is the author of a book on information technology laws and publishes regularly with the Huffington Post. He also serves as a mentor to a number of technology start-ups.

Q. In your experience, do companies in India need to do more to fully understand their data privacy and protection duties in the digital age?

RASTOGI: Companies' approaches to data privacy in India, like elsewhere in the world, are not homogenous. Some have very sophisticated data protection practices, some do not. More importantly, however, Indian data privacy laws are still evolving, and consequently, so are companies' data protection obligations. India recently released its draft Personal Data Protection Bill in July 2018. This bill takes the country one step closer to having a comprehensive data protection regime. Once enacted, it will replace the data protection safeguards under the Information Technology Act, 2000 (IT Act), the current law that governs the collection and use of personal data by companies in the country. The data protection obligations under the bill are stricter than those under the IT Act, and many companies will need to invest more time and resources than they currently do, toward complying with these obligations.

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

RASTOGI: The draft bill is the most crucial development that will affect companies' data processing practices. When enacted, this law will apply to all Indian companies, and some foreign companies, not unlike the European Union's (EU's) General Data Protection Regulation (GDPR). The draft bill, which appears to draw extensively from the GDPR in its current form, might soon be introduced in parliament. We have also seen sector-specific developments. In April 2018, India's financial regulator imposed a hard data localisation mandate on payment systems data, directing that it be locally stored on systems only in India. A government task force set up to frame a now scrapped draft e-commerce policy for India also recommended data localisation. In August 2018, the telecom regulator issued non-binding privacy recommendations for telecom sector data. Most recently, the Supreme Court outlawed the private sector from using Aadhaar, the country's biometrics-based national identification project.

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

RASTOGI: India's current data protection law – the IT Act – is limited in scope, and largely only protects individuals' sensitive personal data. Criminal statutes provide the framework for the monitoring and enforcement of crimes, such as stalking, harassment and identity theft, that could threaten the privacy of individuals. In order to tackle the increasing number of such crimes taking place over the internet, the police departments of all states in the country have established cyber security cells and response units. The Union Home Ministry has responded to this shift by announcing the establishment of the Indian Cyber Crime Coordination Centre (I4C), to coordinate cyber crime investigations across the country. The country's forthcoming data protection law will establish a data protection authority, which will be tasked with monitoring and enforcing data protection obligations.

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

RASTOGI: The recent spate of data breaches has played a significant role in the development of a strong data protection framework in India. For example, the data risks exposed by the Facebook-Cambridge Analytica data breach have influenced the work of the Committee of Experts on Data Protection Framework for India, which drafted India's draft data protection bill. The draft bill has incorporated a number of provisions to protect data principals from the threat of data breaches, which is a significant departure from the position in current law. Under the new law, data controllers will be required to notify the new Data Protection Authority (DPA) about personal data breaches, where such breaches are likely to harm a data principal. The DPA can determine if the data fiduciary should inform the data principal about the breach of his or her data, so that the data principal can take measures to mitigate any harm. The DPA can also require the data fiduciary to post the details of any data breach on its website. Further, the draft bill also contains penalties for data fiduciaries which fail to notify the DPA of any personal data breach.

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

RASTOGI: Companies will have to ensure that any third parties they are involved with are compliant with the GDPR, US privacy laws, and the laws of countries they do business with. Typically, companies will need to ensure such compliance by third parties through contractual undertakings. Since the GDPR came into effect, we have seen a lot of Indian companies, which are third-party service providers, make such contractual representations to EU data controllers. It is also good practice to ensure that third parties comply with international data security standards, such as the ISO 27Ks, SOC and PCI. Proper due diligence should be conducted at the on-boarding stage and at regular intervals to ensure compliance with these data protection standards.

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?

RASTOGI: Companies should secure all data and networks, authenticate users and encrypt all confidential and personal data. As a general

"Companies will have to ensure that any third parties they are involved with are compliant with the GDPR, US privacy laws, and the laws of countries they do business with."

practice, companies should minimise the confidential information stored on portable devices. If any device is lost, the organisation should try to retrieve that data or try to delete it remotely. Maintaining regular backups can help prevent such data losses. GPS trackers can be installed in company laptops and phones to trace them in the event that such devices are lost or stolen. Storing important company data on a cloud server may also prevent data breaches as a result of lost or stolen devices, since passwords of cloud accounts can be changed immediately to prevent data access. Similarly, companies could also request that carriers deactivate services to lost or stolen devices to prevent data access. Built-in encryption devices will also prevent loss of data in the event that a USB, laptop or phone is lost. Other technologies that can be used to prevent data theft or loss are facial recognition, voice recognition and fingerprint locks on devices. ■

www.ikigailaw.com

IKIGAI LAW

ANIRUDH RASTOGI
Founder
+91 98991 44333
anirudh@ikigailaw.com

NEHAA CHAUDHARI
Public Policy Lead
+91 85301 66662
nehaa@ikigailaw.com

TUHINA JOSHI
Associate
+91 81978 19932
tuhina@ikigailaw.com

Ikigai Law is a boutique law and policy firm in India, specialising in representing technology business and investors. The firm is privileged to represent some of the largest technology companies globally and innovative ventures in India, including satellite manufacturers, UAV companies, e-retailers, AR/VR hardware and content companies, crypto-currency platforms and other FinTech ventures. The firm has an active data privacy and protection practice.

China & Hong Kong

JENNIFER HO
PwC Hong Kong
Partner
+852 2289 2919
jennifer.cw.ho@hk.pwc.com

Jennifer Ho is a partner at PwC Hong Kong and leads PwC Hong Kong and China's risk assurance digital risk solutions business, encompassing data governance, data protection, cyber security, data analytics, enterprise system solutions and emerging technologies. She has extensive experience of providing a range of risk management services. She has led engagements, including data governance, data protection, IT security, IT effectiveness, ERP business process optimisation and third-party assurance to enhance trust of organisations operating in the digital world. She has worked across various industry sectors including insurance, retail and consumer, hospitality, public, and energy and utilities.

Q. In your experience, do companies in China & Hong Kong need to do more to fully understand their data privacy and protection duties in the digital age?

HO: The increased pace of digital innovation and the evolving technology landscape, including innovations such as the Internet of Things (IoT), cloud computing, intelligent process automation and artificial intelligence (AI), has created exciting new opportunities, new streams of investment and new sources of revenues. Digital innovation has also led to an elevated risk of data privacy and protection issues. Data breaches have grown exponentially, thus it is more important than ever for companies to safeguard their data and assets. Some companies may not even know that their current business practices are in breach of the relevant data privacy and protection regulations. Companies in Hong and China are required to implement effective controls and security measures to protect not only the personal identifiable information (PII) of their customers, suppliers and employees, but also the information that helps companies to operate, such as research and development (R&D) data, as well as financial and operational data. Failure to put effective controls and security measures in place may result in heavy fines and potentially criminal

liability. It is more important than ever for companies in all sectors to understand their duties and obligations with respect to data privacy and protection.

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

HO: In Hong Kong, the last significant amendments to the Personal Data (Privacy) Ordinance (PDPO) were passed in 2012. However, the Privacy Commissioner for Personal Data (PCPD) continues to be actively involved in the issuance of new and revised non-binding guidelines on the management of personal data. These guidelines intend to serve as practical guidance in respect of any requirements under the PDPO. The enforcement of the European Union's (EU's) General Data Protection Regulation (GDPR) on 25 May 2018 will potentially impact some companies in Hong Kong. In China, in addition to the need to comply with the China Cybersecurity Law, which came into effect on 1 June 2017, companies should also understand the information security technology – personal information security specification – which came into effect on 1 May 2018. Although the specification is not a law, it can be used as a reference by the Chinese enforcement agencies in their enforcement activities.

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

HO: The PCPD has, in recent years, engaged in different regional and international forums, and has joined forces with the global data privacy community, namely the Global Privacy Enforcement Network (GPEN) and the Asia Pacific Privacy Authorities to collaboratively increase data privacy awareness. The Commissioner has also recently participated in a global privacy sweep exercise, conducted by the GPEN on IoT devices. Moreover, the Commissioner has released several code of practice and guidance notes to help companies in Hong Kong to handle data privacy-related matters. Over the past year or so, the Commissioner has issued 25 warnings and three enforcement notices to data users, and referred 19 cases to the police; the majority of these cases were related to direct marketing provisions.

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

HO: In Hong Kong, two recent high-profile data breach cases were investigated by the PCPD. The first case was a data security breach by a major toy manufacturer, which resulted in the theft of 6.6 million records, including parents' names, passwords, children's dates of birth, and so on. The investigation revealed that ineffective security measures were practiced in the handling of personal data. In October 2018, a major airline headquartered in Hong Kong

disclosed a massive data breach which included the personal information of of more than 9 million passengers. The personal data included passenger names, nationalities, dates of birth, phone numbers, email and physical addresses, passport numbers, identity card numbers, frequent flyer programme membership numbers, customer service remarks and historical travel information. The airline has since come under close scrutiny from lawmakers and the public. In China, in August 2018, it was reported that one of the largest data breaches ever was at one of China's leading hotel groups which saw nearly 500 million pieces of personal information and hotel booking details leaked. One important conclusion we can draw from these high-profile data breaches is that not only is it important for a company to have good data protection governance, policies and procedures, as well as controls and security measures, it must also conduct regular, robust data protection reviews to identify issues.

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

HO: Companies often rely on third parties in order to achieve their core business functions, gain competitive advantages and reduce operating costs. The risk can be higher if large volumes of data are processed by the third parties. To mitigate data risks, it is essential for companies to establish a robust third-party risk management (TPRM) programme throughout the lifecycle of the engagement. The programme should involve thorough third-party due diligence prior to the engagement in which the company must understand the nature, scope and purpose of processing as it relates to services performed by third parties, in order to establish an appropriate level of oversight. The relevant data privacy contractual terms and on-site security reviews or independent review of the third-party programmes should be adopted to further mitigate the data security risks arising from the use of third parties.

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?

HO: Research has found that insider threats are often the cause of the biggest security breaches, and they are costly to remediate. It is important to have both effective detection and preventive security measures in place to manage internal risks, as well as access controls which grant employees' access to personal data on a 'need to know' basis. Appropriate incident response planning should also be in place. 'Tone from the top' and awareness training are important. Also, employees should be educated and regularly reminded of their duties and responsibilities in managing personal data and the consequences of failure in protecting personal data. To minimise data protection risks and threats, companies should implement data loss prevention (DLP) tools, processes and controls, and combine these with strategic, operational and tactical measures.

"Research has found that insider threats are often the cause of the biggest security breaches, and they are costly to remediate."

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

HO: A data protection strategy and programme, including a governance model which aligns with a company's vision, goals and risk profile, are critical to identifying and managing data privacy and protection risks. A 'future proof' data protection capability is needed which will enable a company to develop innovative and commercial uses of data, in ways which are fair, ethical and lawful. The commitment and support of senior leaders must be obtained in order to achieve the desired data protection governance model and supporting framework. As data protection regulations are being continuously reformed and getting more stringent, companies should monitor and review their data privacy policies and procedures regularly to ensure compliance with the regulations. It is equally important that there is a cultural shift among companies – they should see data protection and privacy as a business enabler, not just a compliance obligation.

www.pwchk.com

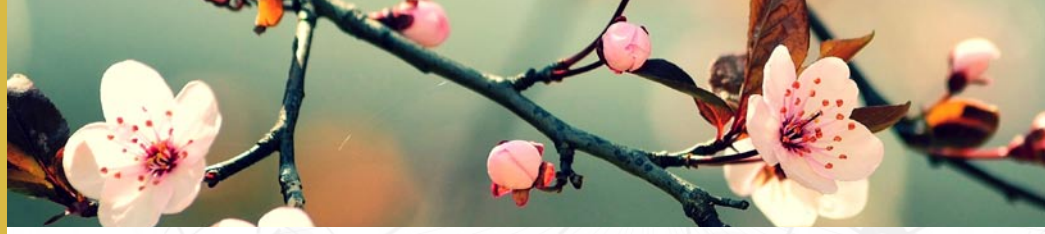
pwc

PwC China, Hong Kong and Macau work together on a collaborative basis, subject to local applicable laws. Collectively, the firms have over 600 partners and over 17,000 people in total. PwC provides organisations with the professional service they need, wherever they may be located. The firm's highly qualified, experienced professionals listen to different points of view to help organisations solve their business issues and identify and maximise the opportunities they seek.

JENNIFER HO
Partner
+852 2289 2919
jennifer.cw.ho@hk.pwc.com

KENNETH WONG
Partner
+852 2289 2719
kenneth.ks.wong@hk.pwc.com

LISA LI
Partner
+ 86 (10) 6533 2312
lisa.ra.li@cn.pwc.com



Japan

TAKASHI NAKAZAKI
Anderson Mori & Tomotsune
Special Counsel
+81 3 6775 1086
takashi.nakazaki@amt-law.com

Takashi Nakazaki is special counsel at Anderson Mori & Tomotsune with broad experience in the areas of data protection and privacy, including Big Data and the Internet of Things (IOT), information security and intellectual property, including copyright and trademarks, licensing and payment services. He also has experience working on matters relating to cyber law issues, such as cloud computing, domain names, e-commerce and social media, computer forensics, digital copyright, software development and open source code, telecommunications, labour and general corporate law.

Q. In your experience, do companies in Japan need to do more to fully understand their data privacy and protection duties in the digital age?

NAKAZAKI: More Japanese companies are receiving personal data from foreign countries while providing online services to foreign consumers and, as such, they are becoming increasingly subject to the data privacy regulations of the consumers' home countries. Accordingly, companies have to comply with cross-border data transfer regulations and be aware of the possible extraterritorial applicability of other regulations. Also, many Japanese companies utilise third-party services, such as cloud computing and data analysis. These services are sometimes provided by foreign entities and, as such, Japanese companies must be aware of the potential risks arising from such a data transfer.

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

NAKAZAKI: From an international perspective, Japan and the European Union (EU) are continuing to negotiate an agreement concerning the cross-border transfer of personal data and will likely reach a final agreement soon – the EU Japan Adequacy Decision. Eventually, it is hoped that the transfer of personal data from Japan to EU countries and vice versa will be possible. With a view to the implementation of this potential agreement, the Personal Information Protection Commission (PIPC), the data protection authority in Japan, issued additional rules regarding the transfer of personal data from EU countries in August 2018 – these rules will apply to all Japanese companies transferring personal data going forward after the Adequacy Decision.

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

NAKAZAKI: The PIPC is the authority governing personal data protection issues in Japan. The PIPC, which was established in January 2014, does not publicise the details of its investigations, though it did make a public announcement concerning administrative guidance it provided to Facebook in October 2018, in relation to a data leak which affected 87 million users in 2016. The PIPC has also announced that it will strengthen cooperation and information exchanges with foreign authorities in the future.

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

NAKAZAKI: In the summer of 2018, a number of Japanese hotels experienced international data breaches and found that they had to report those breaches to the data authorities of EU

countries, regardless of whether those hotels had a presence in EU Member States. Many of the Japanese hotels affected had a hotel reservation website for EU residents and that website was operated by a third-party service provider. Though the incidents occurred under the management of the service provider, the hotels were considered liable. Japanese companies should pay special attention to third-party service provider agreements, particularly with a party in a foreign country, including EU Member States.

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

NAKAZAKI: There have been many data leaks which have arisen from the use of third parties in Japan. It is important to check the security and compliance measures of third parties before beginning a relationship. Also, it is essential that those parties take sufficient measures and report any incident immediately on a contract basis. Companies must monitor whether those measures are being sufficiently implemented. Particularly when dealing with consumer data, it is important for companies to appreciate the gravity of a data incident and respond as quickly as possible, reporting it to the authorities, if necessary.

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?

NAKAZAKI: Many data privacy incidents have arisen out of the loss of devices and data theft by current and retired employees. To avoid such incidents, companies should take both organisational and technological measures. From a technological perspective, it is important to ensure that adequate access control measures are implemented. Employee access must also be monitored. Many companies fail to suspend or terminate data access when an employee leaves the organisation, which can allow unauthorised parties to access data. To mitigate these risks, companies should introduce robust data encryption procedures and remote control systems, such as disabling data access and data destruction.

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

NAKAZAKI: It is vital that companies educate senior executives and employees alike about the importance of managing data risks and regulatory compliance. It is also important for

"Many data privacy incidents have arisen out of the loss of devices and data theft by current and retired employees. To avoid such incidents, companies should take both organisational and technological measures."

companies to educate senior management about the importance of sufficiently budgeting for the technological and organisational measures required to mitigate the risks rising from data incidents and regulatory breaches. To educate employees, companies should establish internal corporate rules, including strict disciplinary actions for breaches and provide regular educational exercises. Parties should also conduct tests of their personnel and systems. It is also very important to implement these measures on a company-wide basis, not just within IT or compliance departments. ■

www.amt-law.com

ANDERSON MŌRI & TOMOTSUNE

Anderson Mori & Tomotsune is a full-service law firm formed by the winning combination of three leading law firms in Japan. The firm provides an extraordinarily powerful value proposition. The firm has the capability to serve a multinational client base, advise on inbound, outbound and domestic projects and provide expert, timely and cost-efficient advice across a full range of legal issues.

TAKASHI NAKAZAKI
Special Counsel
+81 3 6775 1086
takashi.nakazaki@amt-law.com

Singapore

JENNIFER CHIH
PK Wong & Associates LLC
Director
+65 6827 5552
jennifer.chih@pkw.com.sg

Jennifer Chih leads the firm's data protection practice area. A Singapore-qualified lawyer with over 20 years of experience in the profession, her areas of expertise include data protection law, corporate law, employment and immigration law. Given the increasingly global nature of data flows, she has been deeply involved in cross-border projects involving data transfers between various countries. Keenly aware of the challenges companies face putting data protection into practice, Ms Chih frequently conducts training for in-house counsel, compliance officers and employees.

Q. In your experience, do companies in Singapore need to do more to fully understand their data privacy and protection duties in the digital age?

CHIH: Companies in Singapore are increasingly aware of their duties in relation to data privacy and protection. However, there remains much room for improvement. While many businesses have put in place data protection policies and appointed data protection officers, compliance is often formulaic. Many businesses still fail to understand that data protection requires a continuing effort and that data protection measures need to be embedded into each business' practices and processes. In addition, with the blurring of geographical lines, businesses sometimes fail to grasp that the data privacy and protection laws of other jurisdictions may also apply to their operations. In particular, with Singapore and the European Union (EU) having signed a free trade agreement (FTA) this year, Singapore businesses which seek to take advantage of the new trade deal to market to EU consumers will have to ensure that they can comply with the EU's General Data Protection Regulation (GDPR).

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

CHIH: The Personal Data Protection Commission (PDPC), Singapore's personal data protection authority, recognises the changing digital landscape and has proposed several amendments that it intends to make to Singapore's existing data protection framework in the near future. Notably, the PDPC has announced that it intends to merge the Do-Not-Call (DNC) provisions in the Personal Data Protection Act (PDPA) with the Spam Control Act (SCA) under new comprehensive legislation which will govern all unsolicited commercial messages. Cognisant of technological developments, the new regulatory framework will also cover unsolicited commercial messages sent in bulk via instant messaging platforms, and the use of random address generators or address harvesting software for sending commercial messages will be prohibited. Businesses should also take note that the period for effecting requests for withdrawal of consent for sending any commercial messages will be reduced to 10 business days.

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

CHIH: The PDPC has proposed the introduction of a mandatory data breach notification regime. As it stands, there is no mandatory obligation for organisations in Singapore to notify the PDPC or affected individuals in the event of a data breach. Under the PDPC's proposed changes, organisations will have to notify affected individuals as soon as practicable. The PDPC will also need to be notified as soon as practicable, but no later than 72 hours, if a data breach poses any risk of harm to the affected individuals or involves 500 or more individuals. This proposed regime will allow the PDPC to more effectively monitor for large scale breach incidents and provide guidance for post-breach remedial actions.

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

CHIH: This year, Singapore experienced its worst ever data breach when the personal information of 1.5 million patients was stolen in a cyber attack on SingHealth, Singapore's largest group of healthcare institutions. The stolen personal information included sensitive personal data such as national identification numbers and medical records. A committee of inquiry was promptly convened to investigate the incident and the inquiry is ongoing. With the wide media exposure, this data breach has had the positive effect of raising awareness among the general public and organisations – public and private – of the issues around data protection and the importance of responsible processing. One aspect of the incident which has received considerable attention has been the lacklustre efforts by those responsible for addressing the breach when it was first detected. This has highlighted the need for organisations to put in place effective procedures and clear reporting lines for dealing with such incidents.

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

CHIH: Companies should ensure that they perform basic due diligence and check that vendors or business partners are able to comply with the PDPA where personal data is processed. Under the PDPA, organisations in Singapore remain responsible for any personal data which is processed on their behalf even if such processing is performed by a third party. Our experience has been that many businesses remain unaware of this and consequently fail to carry out even basic checks on whether their vendors and business partners are compliant with data protection obligations. In relation to this, many companies also often fail to ensure that their business contracts contain data protection provisions which clearly designate each party's data protection responsibilities.

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?

CHIH: There are several steps that companies can take to address internal data protection risks. As a general principle, companies should endeavour to restrict access to personal data on a need-to-know basis to reduce the extent of any potential breach. Companies should also ensure that their internal corporate policies clearly set out employees' obligations in relation to the handling of personal data. Employee contracts should contain binding confidentiality clauses which protect personal data in the company's possession and procedures should be in place to prevent employees from misusing personal data which they handle. These policies should be easily accessible, brought to the employees' attention and written in plain language. While it is difficult to ensure day-to-day compliance by employees, conducting induction courses and training can help employees better understand their role and reduce risk. For completeness, regular audits should be conducted to check that corporate policies are carried out properly.

"Companies need to embrace the digital age and take proactive steps to lead the way in responsible data processing."

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

CHIH: Data protection is a new but ever-growing area of compliance. However, due to the costs involved, companies sometimes neglect or overlook their data protection obligations, and instead prioritise other more 'traditional' business concerns. With companies processing ever larger amounts of data for business purposes, the risks posed by a potential data breach similarly increase. Cross-border transactions may involve an additional layer of data protection obligations. Notwithstanding the regulatory penalties which may be imposed, organisations involved in data breaches also often face adverse media publicity. With the general public becoming increasingly aware and concerned with data protection issues, companies need to correspondingly prioritise data protection compliance. A reactive form of compliance will result in piecemeal corporate policies which will require continuous fine-tuning and may end up incurring more costs. Companies need to embrace the digital age and take proactive steps to lead the way in responsible data processing.

www.pkw.com.sg

PK WONG & ASSOCIATES LLC

PK Wong & Associates LLC is a medium-sized law corporation that provides a full and varied range of legal services to its clients, catering to every aspect of their needs. The firm's clients range from small businesses to large multinational corporations, and their businesses involve areas such as infrastructure and communication, resort development, construction and many others. Committed to delivering fully integrated services to each of its clients, the firm prides itself on taking an innovative approach to problem solving and effective management of its clients' legal affairs.

JENNIFER CHIH
Director
+65 6827 5552
jennifer.chih@pkw.com.sg

JOHN KUAH
Privacy & Data Protection Leader
+65 6827 5554
john.kuah@pkw.com.sg

MARIA CHANG
Associate
+65 6950 2384
maria.chang@pkw.com.sg

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

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.

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

www.financierworldwide.com