DATA PROTECTION & PRIVACY LAWS

ANNUAL REVIEW **2019**

FINANCIER WORLDWIDE corporatefinanceintelligence

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

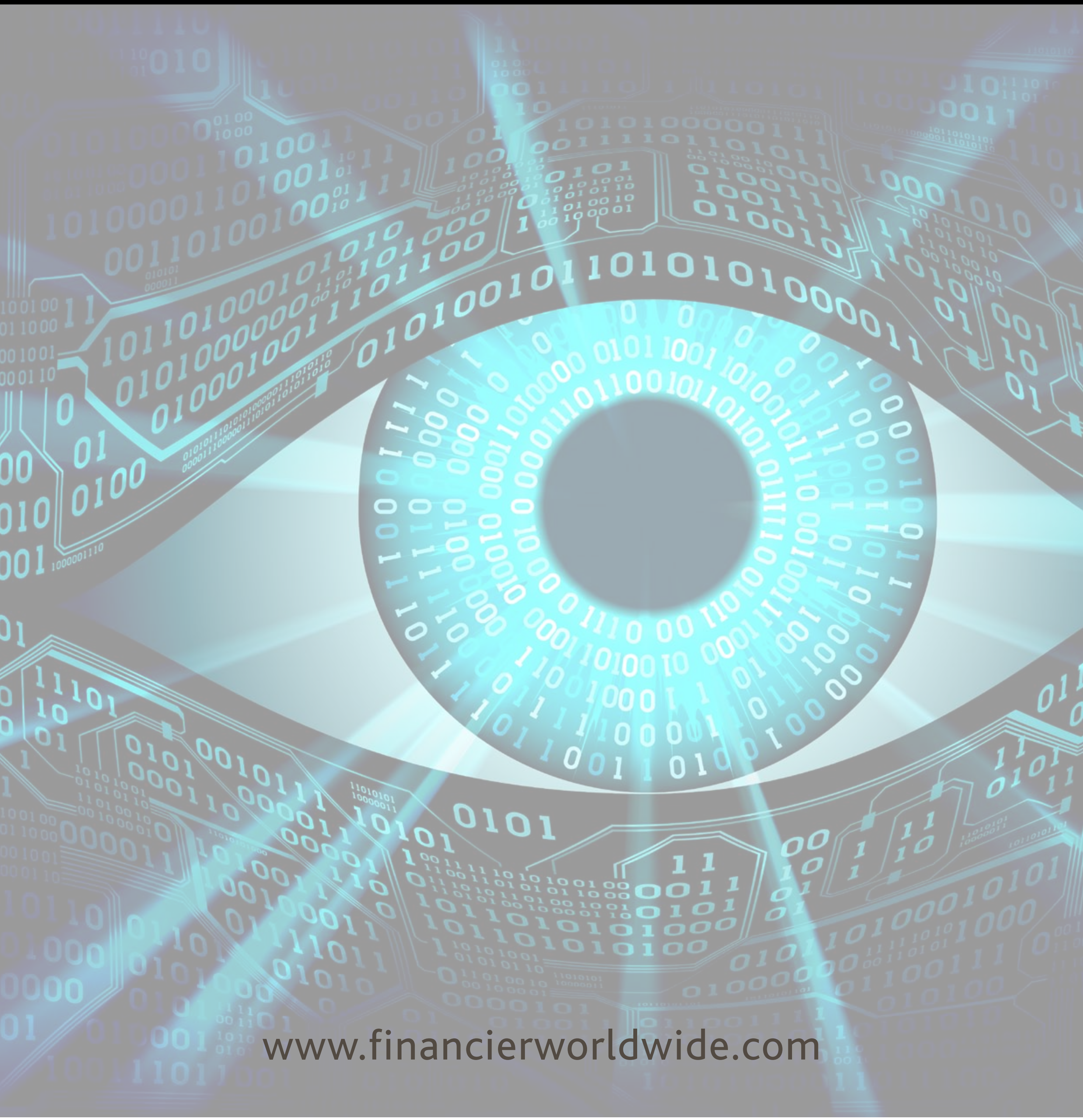
Telephone: +44 (0)845 345 0456
Fax: +44 (0)121 600 5911
Email: info@financierworldwide.com

www.financierworldwide.com

Annual Review • December 2019
Data Protection & Privacy Laws

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

Contents


www.financierworldwide.com

Contents

INTRODUCTION

Data protection is one of the most important issues of our time. There is a burgeoning understanding, among the general public, across business and throughout the world, of the importance of data and the consequences of a breach. The financial and reputational damage suffered by companies that fall short can be significant, particularly since implementation of new legislation such as the European Union's General Data Protection Regulation (GDPR).

The data protection landscape is rapidly changing, so it can be challenging for companies to keep up to date with their compliance obligations. As new legislation emerges, such as the California Consumer Privacy Act (CCPA), the onus is on companies to adapt.

Companies need to understand the data they hold. This can be achieved by conducting a comprehensive, detailed review of the data they collect, including jurisdictions of origin, how it is processed and who processes it. Companies should also provide training to employees on data privacy and cyber security to raise awareness of their data protection obligations.

Given the increasing attention on data protection, companies that fail to take the necessary steps could face dire consequences.

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 (M&As). 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. Do you believe companies fully understand their duties of confidentiality and data protection in an age of evolving privacy laws?

COHEN: Given the rapidly changing privacy landscape in the US, it can be challenging for companies to feel that they fully understand all of their duties, particularly under new legislation for which compliance norms have not yet been established. That said, larger companies that have dedicated privacy personnel who are able to focus on these matters daily are aware of the requirements, particularly in regulated industries. Smaller companies that have fewer resources to devote to monitoring changing requirements may have a harder time keeping up. One argument for general federal privacy legislation is to streamline the compliance process to make it easier for both large and small companies to understand and comply with their privacy obligations.

Q. As companies increase their data processing activities, including handling, storage and transfer, what regulatory, financial and reputational risks do they face in the US?

COHEN: At a time when companies are processing increasing amounts of data, we are seeing a trend in states expanding the types of personal data that are regulated. In addition, some states have updated their data protection laws such that they apply to any company's use of regulated data, without regard to the location of the company. All these elements combine to create more opportunities for companies to run afoul of state data protection laws. New York recently passed the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act), which is an example of each of these trends. The SHIELD Act expands both the definition of personal information and the companies to which data breach reporting requirements apply. Under the SHIELD Act, any company, regardless of whether it conducts business in New York, must notify affected New York residents in the event of a breach of such residents' private information, including breaches involving a resident's payment card numbers, biometric information or email account username and password. The SHIELD Act also increases the penalties for knowing or reckless failure to comply with these data breach notification requirements to $20 per instance, up to a cap of $250,000.

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

COHEN: Under the SHIELD Act, companies that collect private information from New York residents must use reasonable efforts to safeguard it. Failure to comply with the data security provisions of the SHIELD Act can result in penalties assessed by the attorney general of up to $5000 per violation, which penalties are not subject to a cap. Because the SHIELD Act is relatively new legislation, there is currently little guidance on what constitutes a single violation for purposes of this fine. In addition, under New York's newly enacted Identity Theft Prevention and Mitigation Services Act, New York consumer credit reporting agencies that suffer a data breach involving social security numbers must provide five years of identity theft protection to affected consumers. While this requirement is not a penalty per se, it is an example of the type of obligations and expenses that may be imposed on companies following a data breach.

Q. What insights can we draw from recent cases of note? What impact have

these events had on the data protection landscape?

COHEN: Two DC Circuit cases decided over the summer, *National Treasury Employees Union (NTEU) v. Office of Personnel Management* and *Jeffries v. Volume Services America Inc*, deepened the circuit split on standing requirements in data breach cases. In the *NTEU* case, the court found that the heightened risk of identity theft resulting from expropriation of birth dates, social security numbers, addresses and fingerprint records in a cyber security breach is sufficient to establish standing. The court held in *Jeffries* that the increased risk of identity theft resulting from the inclusion of all 16 digits of a customer's credit card number on a receipt, in contravention of the Fair and Accurate Credit Transactions Act, satisfied the plaintiff's standing requirement. These two cases bring the DC Circuit in line with the Third, Sixth, Seventh and Ninth circuits, which have held that victims of data breaches can establish standing by showing a heightened risk of future misuse of their stolen information. The First, Second, Fourth and Eighth circuits have ruled that plaintiffs must show actual harm. Considering this ongoing circuit split, the outcome of data breach litigation continues to be heavily influenced by the jurisdiction in which a case is filed.

Q. In your experience, what steps should a company take to prepare for a potential data security breach, such as developing response plans and understanding notification requirements?

COHEN: First, it is important that companies maintain a comprehensive and detailed description of the categories of data collected by the company, including the jurisdiction of origin and the ways in which it is processed, whether it is processed by the company or its vendors. In a large company, this can be a significant undertaking as there is often no central repository for this type of information. Companies should have a detailed security incident response plan in place that includes, as a minimum, a description of how and when to use the plan, including different levels of incident response and escalation points, the identification of key team members and their roles, categorisation and prioritisation of different types of incidents, plans for each incident type and a plan for communications with third parties. The plan should reflect a company's actual organisational structure and procedures as a plan that is suitable for one company may not necessarily work for another.

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

COHEN: Companies should implement mandatory data privacy and cyber security training for all employees to make sure that each employee understands his or her role in preventing data privacy violations. The training should emphasise the prompt reporting of any unauthorised activity of which an employee may become aware, such as a rogue employee downloading data onto a personal device, as well as the importance of not sharing passwords, even with fellow employees. 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 rogue employee using such data for unauthorised purposes.

"It is important that companies maintain a comprehensive and detailed description of the categories of data collected by the company, including the jurisdiction of origin and the ways in which it is processed, whether it is processed by the company or its vendors."

Q. Would you say there is a strong culture of data protection developing in the US? Are companies proactively implementing appropriate controls and risk management processes?

COHEN: In New York, there is certainly an increased awareness of data protection issues, which is likely due to several factors. First, because New York is a global financial centre, many companies doing business in the state are relatively large, sophisticated organisations which have the resources to dedicate to data protection compliance. In addition, many such companies also have a presence in Europe and have become familiar with data protection issues through their General Data Protection Regulation (GDPR) compliance processes. Second, New York state has been active in implementing new legislation, including the SHIELD Act, to respond to changing data protection needs. Finally, companies in New York are likely influenced by the larger national conversation regarding data protection issues, including news reports regarding high-profile data breaches, the passing of the California Consumer Privacy Act (CCPA) and discussions regarding the possibility of general US federal privacy legislation. Combined, these factors are influencing many companies to take steps to minimise their exposure to data-related incidents and claims.

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

Canada

DAVID KREBS
Miller Thomson LLP
Counsel
+1 (306) 667 5632
dkrebs@millerthomson.com

David Krebs has a business law practice with particular focus on privacy and cyber security, technology and compliance. He is a key contact for Miller Thomson's cyber security practice and is the editor of the firm's cyber security blog. With a background in the life sciences, health, biotech and technology sectors he has hands-on experience in the US, Europe and other cross-border settings.

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

KREBS: I believe that some companies do understand their duty while others are quite unaware of their obligations and the potential risk of exposure they have. For example, the Office of the Privacy Commissioner of Canada (OPC) just released a report summarising the changes in breach reporting since mandatory reporting was implemented in November 2018. The OPC found that the majority of reports relate to unauthorised access. Now, some of this was access by outside bad actors but a large portion of it was access from within, such as employees with improper data access permissions looking at what they were not supposed to be looking at. This is evidence that many Canadian companies are either unaware of their safeguarding obligations or are not taking proactive steps to map, segment and limit access to their data. Either way, they are now faced with a regulatory regime that requires reporting and notification after an incident, which should inspire a better-informed and more forward-thinking approach. Not to mention the potential impact that laws of foreign jurisdictions may have on Canadian companies – most notably, the California Consumer Privacy Act (CCPA) and the European General Data Protection Regulation (GDPR).

Q. As companies increase their data processing activities, including handling, storage and transfer, what regulatory, financial and reputational risks do they face in Canada?

KREBS: Privacy-related class action lawsuits are increasing in Canada. These suits have met mixed results at the certification stage, and thus far, no privacy class action has been determined on the merits. With mandatory breach reporting in effect, and looking to US litigation as a harbinger, this type of class action exposure is likely to increase in Canada. The implementation of mandatory breach reporting and notification is also likely to bring more incidents to light, forcing Canadian businesses to engage in reputational damage control at an early stage. One must also remember that while Canada has a federal privacy law, there are a number of provinces with their own private sector privacy legislation that, while similar, can carry slightly different obligations and apply differently across sectors. As for reputational concerns, Canadians are quite tuned into the risks data intrusion, data loss and surveillance can pose to their personal information. The 2019 breaches at Capital One and Desjardins which exposed millions of records are certainly part of the reason for that.

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

KREBS: Most organisations operating in any province or territory in Canada are subject to privacy legislation, sometimes both federal and provincial. There are exceptions for non-profits and charities in some instances, but one should not rely on those implicitly. Failing to comply with data and privacy laws can result in significant costs to an organisation, including legal costs involved in responding to an investigation and the potentially resulting findings of the regulator, as well as actual fines. For example, failing to comply with breach reporting requirements can result in an indictable offence and in a fine of up to $100,000. Additionally, the individual whose information was subject of the privacy breach can bring an application to the court for a hearing regarding the complaint. Following this

hearing, the court may order remedies, such as requesting that an organisation correct its practices, ordering the organisation to publish a notice of any action taken to correct its practices, and may award damages to the individual. There is currently much debate in Canada about the need to reform Canada's privacy laws and to strengthen the regulator's enforcement powers. I would generally expect those powers, including the ability to levy higher penalties, to increase with any potential changes to Canada's privacy legislation.

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

KREBS: Recently, two massive data breaches occurred affecting millions of Canadians. This past June, the Desjardins Group was victim of a data breach when an employee allegedly leaked private information to outside sources. This breach affected at least 4.2 million individuals. Similarly, Capital One Financial is the subject of one of the largest security breaches in Canadian history with nearly six million individuals being affected due to the actions of one hacker. Both incidents have resulted in major investigations by the OPC. The result of these investigations is likely to have a significant impact on how Canada's current laws are being interpreted. Even though, in both situations, the individuals responsible for the attacks have been identified, this does not prevent the compromised information from being inappropriately used.

Q. In your experience, what steps should a company take to prepare for a potential data security breach, such as developing response plans and understanding notification requirements?

KREBS: Having a plan in place is crucial. This should include knowing who to call and what the immediate next steps should be. Panic is bad but so is inertia. An organisation should contact its breach coach and the rest of the breach response team to come up with a clear tactical plan. If no such plan exists, an ad-hoc team consisting of your in-house counsel, if you have one, IT manager, PR and communications and external legal counsel should be gathered. You may need to call on external IT forensics and incident response experts. If you have insurance, a decision about whether to invoke is another consideration. Understanding notification requirements is obviously important. To do that, you need to understand which requirements apply to your operations, and that may require an analysis of the data impacted.

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

KREBS: It is extremely important for companies to prevent their employees from misusing personal data. In a recent British Columbia case, *Ari v Insurance Corporation of British Columbia* (2019), the court held that an organisation, which had a history of employees leaking private data, may be liable for punitive damages, even though the previous breaches did not relate to the breach at issue. To prevent the misuse of data by rogue employees, organisations can implement tactics such as having a system where each employee is aware that he or she is tracked when accessing personal information, only allowing a few employees access to personal

> *"There is currently much debate in Canada about the need to reform Canada's privacy laws and to strengthen the regulator's enforcement powers."*

information, including data protection in employment agreements and ensuring employees are aware there are serious consequences for leaking private data. If data is misused by a rogue employee, it is important for organisations to deal with the breach appropriately.

Q. Would you say there is a strong culture of data protection developing in Canada? Are companies proactively implementing appropriate controls and risk management processes?

KREBS: As news stories involving massive breaches of personal data become more common, there is a clear shift in culture regarding the protection of personal information. Organisations are actively implementing risk management processes, such as mandating employees to complete practical cyber security awareness modules and other programmatic elements, such as written policies and procedures and investment in IT to support data security. The dawn of the GDPR has also contributed to increased awareness among Canadian companies, both for those who are subject to it but also on a more general level. The GDPR is also having an effect on how the Canadian regulator views Canada's current enforcement regime which, compared with the GDPR, is quite anaemic.

www.millerthomson.com

MILLER THOMSON
AVOCATS | LAWYERS

Miller Thomson is built to provide the most comprehensive Canadian business and legal help. The scale of an organisation's project is never an issue. The firm helps businesses of every size, entrepreneurs and individuals, working with not-for-profit organisations, as well as financial institutions and governments. Miller Thomson's mastery of Canadian law is available to domestic and international clients alike. With close to 550 lawyers and deeply rooted in communities across Canada, the firm has 12 strategically placed offices in Vancouver, Calgary, Edmonton, Saskatoon, Regina, London, Kitchener-Waterloo, Guelph, Toronto, Vaughan, Markham and Montréal.

DAVID KREBS
Counsel
+1 (306) 667 5632
dkrebs@millerthomson.com

ERIC S. CHARLESTON
Associate
+1 (416) 595 8617
echarleston@millerthomson.com

ALICIA MACNEIL
Articling Student
+1 (780) 429 9471
amacneil@millerthomson.com

United Kingdom

TIM HICKMAN
White & Case
Partner
+44 (0)20 7532 2517
tim.hickman@whitecase.com

Tim Hickman advises on all aspects of UK and EU privacy and data protection law, from general compliance issues, such as implementing privacy policies and consent forms, to more specialised issues, such as managing data breaches, structuring cross-border data transfers and complying with the 'right to be forgotten'. He has a detailed knowledge of the EU's General Data Protection Regulation (GDPR), and co-authored White & Case's Handbook on that piece of legislation. He has significant experience of working with a wide range of clients in the EU, Asia and the US.

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

HICKMAN: The degree to which different businesses understand their data confidentiality and data protection obligations varies significantly. In part, this is a result of sectoral differences – businesses that have historically experienced high volumes of complaints from individuals regarding the processing of personal data, such as technology companies, healthcare providers, and so on, generally have a deeper understanding of these issues simply because they have been forced to grapple with them more frequently. In addition, businesses in highly regulated sectors, particularly the financial services sector, tend to benefit from existing compliance infrastructure onto which data protection compliance can be added relatively easily, whereas businesses in less regulated sectors tend to require greater initial investment in order to get up to speed. The general level of understanding of these issues has been poor, historically, but has begun to improve, with the advent of new and well-publicised laws, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Q. As companies increase their data processing activities, including handling, storage and transfer, what regulatory, financial and reputational risks do they face in the UK?

HICKMAN: Any business that handles personal data is exposed to the risk that affected individuals might bring claims for compensation if the business misuses the data or fails to keep it secure. While the damages per claimant are likely to be low, the GDPR creates the possibility of quasi-class actions, which could have significant adverse financial consequences for affected businesses. In addition, there is obvious potential for damage to the reputation of a business if it is found to have breached the GDPR. It should be noted that the outcomes of investigations into breaches of the GDPR are, in most cases, permanently published on the websites of the relevant regulators, and those pages tend to be highly ranked in search engines and are commonly frequented by journalists and investors. As a result, the reputational consequences of non-compliance can be significant.

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

HICKMAN: Breaches of the GDPR carry the potential for fines of up to the greater of €20m or 4 percent of worldwide turnover. Although these powers are generally reserved for particularly serious cases, it is important to note that they do not require a business to intentionally breach the GDPR. EU regulators have issued multi-million euro fines for breaches of the GDPR that were negligent, rather than deliberate. It should also be noted that the quantum of such fines is often not covered by insurance policies. In addition, EU regulators have the power to order businesses to cease processing activities where the regulators consider those activities to be contrary to the GDPR. While this power is unlikely to be used regularly, its potential consequences would be significant for any business that is ordered to cease or suspend business-critical processing activities.

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

HICKMAN: A major misconception in the past was that the GDPR was mostly aimed at large, consumer-facing technology businesses, and that businesses in other sectors faced lower levels of risk. However, the UK Information Commissioner's Office (ICO) dispelled that view earlier this year by publishing notices of intent to issue fines totalling more than £250m to a hospitality company and an airline. All businesses are increasingly reliant on technology for the purposes of their day-to-day operations, and that technology brings with it significant advantages, notably in respect of the ease with which information can be moved, and the speed at which commerce can be conducted. However, it also brings significant risks, in the form of the heightened likelihood of data breaches. As a result, businesses in all sectors are beginning to realise that implementing and maintaining appropriate data protection and cyber security measures is simply a necessary cost of doing business.

Q. In your experience, what steps should a company take to prepare for a potential data security breach, such as developing response plans and understanding notification requirements?

HICKMAN: The first step that businesses need to take in preparing for the risk of possible data breaches is to accept that the risk is real. Far too many businesses assume that because they have not suffered a breach yet, as far as they are aware, they never will. Unfortunately, that view simply makes data breaches more likely. The second step is to make appropriate investments in data protection compliance, data security and employee training, as these are three areas in which incremental improvements can significantly reduce the risk of attacks. The third step is to put in place appropriate data breach response plans setting out the recommended steps for dealing with a data breach, and the applicable internal and external reporting requirements. Those rules should include fall-backs and alternatives at every stage, so that the absence or unavailability of a team member does not prevent the data breach from being appropriately escalated, resolved and reported.

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

HICKMAN: The most overlooked data breach risks often come from well-meaning employees who are just trying to do their jobs, but who are boxed in by IT security restrictions that are not well-suited to the operational needs of the business. This commonly leads such employees to invent workarounds that can create a much greater risk than the one against which the IT security restrictions were originally intended to protect. For example, some businesses have deactivated USB drives on employee laptops, which has resulted in employees storing data in non-secured cloud accounts. Some of those businesses have gone on to block all access to cloud services, which has resulted in employees forwarding data to their private email accounts. If over-restrictive IT security measures are implemented, employees will develop ways around them, so that they can keep doing their jobs. Consequently, in addition to ensuring that employees are properly trained on data protection and cyber security, businesses need to ensure that their IT security measures are properly tailored to the relevant business functions, so that employees are not unnecessarily impeded in their daily work.

> *"The first step that businesses need to take in preparing for the risk of possible data breaches is to accept that the risk is real."*

Q. Would you say there is a strong culture of data protection developing in the UK? Are companies proactively implementing appropriate controls and risk management processes?

HICKMAN: The culture of data protection among businesses in the EU is developing, but it is a slow process. As individuals become more aware of their rights, and as businesses are more exposed to the consequences of non-compliance, there is a gradual increase in awareness and expertise. However, there are significant challenges to overcome. Under the GDPR, regulators have vastly more data breach reports to work through than they did under the previous regime. At the same time, they are facing stiffer competition from the private sector for talented and experienced staff. As a result, many regulators have been over-stretched, which means that the resources available for enforcement have been limited. Consequently, for most businesses, the likelihood of enforcement in this area is relatively low. At the same time, the cost of full compliance with the GDPR can be significant, and many businesses have therefore reached the conclusion that achieving full compliance is simply not worth it. It will take time for businesses to come fully into line with the applicable legal requirements.

TIM HICKMAN
Partner
+44 (0)20 7532 2517
tim.hickman@whitecase.com

Germany

KATHRIN SCHÜRMANN
Schürmann Rosenthal Dreyer
Partner
+49 (0) 30 2130 0280
schuermann@srd-rechtsanwaelte.de

Kathrin Schürmann has been a partner at Schürmann Rosenthal Dreyer since 2007 and specialises in IT and data protection law, as well as competition law. A particular focus of her practice is on advising companies in the fields of digital business, technology and the media. In her function as a data protection expert, Ms Schürmann focuses on national and international clients in the introduction and development of new digital business models.

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

SCHÜRMANN: Much has changed in recent years in terms of understanding and appreciating data protection, both among companies and individuals. A driving factor in this change was undoubtedly the implementation of the General Data Protection Regulation (GDPR) in May 2018, which forced companies to become more aware of their own data processing practices and their implications. However, this process is still relatively new and will require constant maintenance and further development, particularly for data-driven business models. The past has also shown that scandals in connection with data protection and data security can cause lasting damage to a company's reputation. Companies should therefore see the further development of data protection law not as a burden, but as an opportunity to make their own data-driven processes more efficient and secure, which is necessary to gain the trust of their customers. Trust and the responsible handling of data will be a key competitive advantage for companies in the coming years.

Q. As companies increase their data processing activities, including handling, storage and transfer, what regulatory, financial and reputational risks do they face in Germany?

SCHÜRMANN: The introduction of the GDPR has significantly increased government pressure on companies to comply with appropriate data protection standards. In Europe, severe penalties, such as those issued by the British Information Commissioner's Office (ICO) against British Airways, an airline whose core business model is not the processing of data, have been imposed and monitored by companies. In Germany, real estate company Deutsche Wohnen was recently fined several million euros for a breach of data protection laws. Undoubtedly, data protection is becoming increasingly important from a consumer perspective, and, of course, for businesses, as the recent fines increase the fear of being 'next'. In Germany, a great deal of importance is placed on corporate reputation and data protection, yet despite the significant penalties imposed, reputational damage can often weigh more heavily on companies.

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

SCHÜRMANN: The GDPR allows penalties of up to €20m or 4 percent of the annual worldwide turnover of the preceding financial year, whichever is higher. The specific penalty imposed depends on many factors. Including the willingness of businesses to cooperate with the data protection authority and the number and seriousness of data protection breaches. Furthermore, in different EU countries different penalty practices have developed, therefore there have been efforts to harmonise the calculation of penalties. In general, however, the longer the GDPR is in force, the less lenient the authorities will be and the higher their expectations of data protection standards will be. Recently, there has been a rapid increase in both the number and amount of penalties imposed.

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

SCHÜRMANN: In the Deutsche Wohnen case, personal data of customers were not deleted but stored significantly longer than necessary for business purposes. The Deutsche Wohnen case shows that every company that maintains databases containing personal data of its customers must deal not only with its security but also with the necessity and duration of data storage. The Deutsche Wohnen case was aggravated by the fact that a plan for data retention and deletion was not drawn up and implemented. It is therefore important for companies to proactively check their databases and processes for data protection compliance. Otherwise it can be difficult to implement the requirements of the data protection authority on time. The effects on the data protection landscape are a sharp increase in the budgets and activities around GDPR implementation. Many companies, after the initial implementation of the GDPR, have not pushed this sector as actively.

Q. In your experience, what steps should a company take to prepare for a potential data security breach, such as developing response plans and understanding notification requirements?

SCHÜRMANN: A company should determine the steps to be taken in the event of a data protection incident before any breach occurs. This is particularly important as the GDPR provides strict deadlines for reporting data protection incidents – 72 hours – non-compliance with which can lead to substantial fines. Accordingly, it is important to train those employees who regularly deal with personal data how to handle such cases, who to inform, and so on. It is also helpful to implement standardised processes and clear responsibilities to ensure that the right people in the organisation are aware of the incident and know how to respond.

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

SCHÜRMANN: It is important that companies have authorisation processes in place governing access to personal data. In principle, every employee should only be able to access the data needed to perform his or her daily tasks – the 'need to know' principle. It is also important to have physical access controls and a clean desk policy in place. This is not only advisable from a data protection perspective, it is also

"Companies should always see data protection as an opportunity to develop further, gain the trust of their customers and not just as a bureaucratic hurdle which must be cleared."

helpful to preserve the business secrets of the company. A further element is encryption and pseudonymisation, through which only a small number of employees have access to the actual personal data.

Q. Would you say there is a strong culture of data protection developing in Germany? Are companies proactively implementing appropriate controls and risk management processes?

SCHÜRMANN: In Europe, and particularly in Germany, a data protection culture is beginning to form faster. Not only since the introduction of the GDPR companies recognised the value of data protection and data security for the protection of their business secrets, against official penalties and not least the personal data of their customers. For this reason, many companies have already developed or are working on comprehensive data protection concepts. In addition, data protection forces companies to be aware of their internal processes and, if necessary, to adapt and optimise them. For this reason, companies should always see data protection as an opportunity to develop further, gain the trust of their customers and not just as a bureaucratic hurdle which must be cleared.

www.srd-rechtsanwaelte.de

SCHÜRMANN ROSENTHAL DREYER
RECHTSANWÄLTE

Schürmann Rosenthal Dreyer is a firm which stands up for its clients. The firm thinks in solutions, not of them. Digital business models are the firm's core competencies, with IT law, data protection law, intellectual property, copyright and media law, trade and distribution the firm's areas of expertise. The firm's lawyers are leaders in their fields and deliver solutions for their clients that enable them to expand their market advantage.

KATHRIN SCHÜRMANN
Partner
+49 (0) 30 2130 0280
schuermann@srd-rechtsanwaelte.de

Italy

GIANGIACOMO OLIVI
Dentons
Partner, Co-Head of Europe Data Privacy and Security
+39 02 726 268 00
giangiacomo.olivi@dentons.com

Giangiacomo Olivi is a partner in Dentons' Milan office, Europe co-head of the Data Privacy and Cybersecurity group and Europe co-head of the Media Sector group. He is a member of the global Intellectual Property and Technology practice. He assists clients, such as national and international companies as well as industrial associations, providing strategical and commercial legal advice in relation to technology, media and communications matters, with a specific focus on data management. He also assists clients with regard to outsourcing and commercial transactions in a wide range of sectors.

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

OLIVI: Based on our professional experience, companies' awareness of confidentiality and data protection has significantly evolved in recent years. The European Union (EU) General Data Protection Regulation (GDPR) has had a fundamental role in strengthening companies' data protection culture and in granting a higher level of attention to personal data processing. That said, the path of growth in the field of privacy is at an early stage and data protection provisions are still evolving. In this context, the role of legal advisers is essential to further raise awareness and help companies to fully understand their confidentiality and data protection duties.

Q. As companies increase their data processing activities, including handling, storage and transfer, what regulatory, financial and reputational risks do they face in Italy?

OLIVI: The so-called data-driven economy is characterised, among other things, by massive

processing of personal data – Big Data – using new technologies, such as artificial intelligence (AI). It is clear that the more personal data a company processes, the more a personal data breach, such as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, is likely to occur and the greater a company's regulatory duties and reputational risks are. The implementation of appropriate technical and organisational measures, such as confidentiality, integrity, availability and resilience of processing systems, pseudonymisation and encryption of personal data, and regular penetration tests, will ensure a level of security appropriate to the risk.

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

OLIVI: The Italian Data Protection Code provides a hybrid punitive framework based on both administrative fines and criminal penalties. As to the former, the same GDPR administrative fines apply – up to €20m and 4 percent of total worldwide annual turnover. It is up to the Italian Data Protection Authority (Garante) to assess and estimate the applicable administrative fine, on a case-by-case basis. As for criminal penalties, which consist of imprisonment ranging from six months to six years, they apply to certain specific behaviours, such as unlawful communication and dissemination of personal data, fraudulent acquisition of personal data where a large-scale processing takes place, misrepresentations and false declarations to the Garante, and a breach of the Garante's orders.

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

OLIVI: The right to privacy is certainly a 'living matter', subject to continuous updates and evolutionary interpretations. In this context, both national courts and the Court of Justice of the European Union (CJEU), as well as national supervisory authorities, have the role and the responsibility to guide the interpretation and the implementation of the GDPR and all relevant data protection laws and regulations. As a result, case law has actually had a revolutionary impact on the international data protection

landscape and established a new approach with reference to certain provisions. In general, recent cases have in common a greater focus on the protection of the rights and freedoms of natural persons.

Q. In your experience, what steps should a company take to prepare for a potential data security breach, such as developing response plans and understanding notification requirements?

OLIVI: Based on our professional experience, awareness and organisation are the essential requirements for a company to deal effectively with any personal data breach. Such requirements can be met by implementing a data breach policy, which should identify the rules and procedures to be followed in the event of a security incident. Another initiative that every company should undertake to ensure the correct management of a data breach is to organise periodic simulations to identify any inefficiencies.

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

OLIVI: An effective way to prevent internal risks arising from rogue employee conduct is to organise regular training on data protection matters in order to create a strong data protection culture. Employee training is not explicitly required by the GDPR, but it certainly is a way to comply with the well-known accountability principle, according to which the data controller should have, among other things, appropriate measures in place to be able to demonstrate compliance with the GDPR, providing that any individual acting under the authority of the controller who has access to personal data, such as employees, may not process such data unless instructed to do so by the controller himself.

Q. Would you say there is a strong culture of data protection developing in Italy? Are companies proactively implementing appropriate controls and risk management processes?

OLIVI: According to Capgemini Research Institute, only 28 percent of Italian companies are fully compliant with relevant data protection provisions. This percentage denotes a still weak data protection culture. However, companies are experiencing the benefits of data protection compliance – 81 percent of those companies that are in line with the GDPR have acknowledged that it has had a positive impact on reputation and brand image. Garante’s investigations and orders will be of paramount importance to promote companies’ compliance and develop a stronger data protection culture.

"An effective way to prevent internal risks arising from rogue employee conduct is to organise regular training on data protection matters in order to create a strong data protection culture."

www.dentons.com

In today's challenging economy, and with Italy recovering from recession, transactions and projects are best guided by an established and trusted adviser such as Dentons. Italy is known for its innovative and creative businesses, and Dentons' lawyers have been supporting local and international clients in the country for almost two decades. The firm's team will provide access to a comprehensive array of legal support across a broad range of sectors and practices to help clients manage the prevailing economic conditions, to grow and succeed.

GIANGIACOMO OLIVI
Partner, Co-Head of Europe Data Privacy and Security
+39 02 726 268 00
giangiacomo.olivi@dentons.com

India

APRAJITA RANA
AZB & Partners
Partner
+91 (0120) 417 9986
aprajita.rana@azbpartners.com

Aprajita Rana is a partner at AZB & Partners. She has over 10 years' experience of advising clients in areas of technology, data protection, cyber security, telecommunications, white-collar crime and employment. She has been involved in public policy representations on defining the scope of intermediary liability in India and on recommendations for data interception. She has advised leading information technology and financial companies on setting up privacy frameworks for cross-border operations, on cyber incident responses, data protection, encryption standards, consent mechanisms and data localisation. She also advises clients on general commercial and corporate matters across diverse sectors.

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

RANA: Companies are becoming increasingly aware of their duties of confidentiality and data protection, though awareness varies across sectors and businesses. Sectors such as banking, telecommunications, the cloud and e-commerce have witnessed data-focused regulatory intervention and are therefore more aware. The emergence of the General Data Protection Regulation (GDPR) has also contributed to this awareness, as Indian companies that are part of multinational groups or are driven toward EU businesses have been evaluating their data protection frameworks to make them GDPR compliant. India was ranked sixth in GDPR preparedness by a Cisco Data Privacy Benchmark study. In 2018, India released its Personal Data Protection Bill, 2018 (PDP Bill) for public consultation, which will replace the existing privacy landscape under the Information Technology Act, 2000 (IT Act). The extended consultation period encouraged many businesses to identify process gaps in their compliance. Businesses are aware that once the PDP Bill is notified, they will need to devote time and resources to manage their exposure.

Q. As companies increase their data processing activities, including handling, storage and transfer, what regulatory, financial and reputational risks do they face in India?

RANA: With India on the cusp of a new data privacy regime, the risks associated with existing data processing and the related compliance requirements will increase manifold. Most business activities are driven toward customer generation and retention, and therefore the risks will apply across a range of activities. Companies will not be able to rely on template practices and will have to examine each stage of data processing and its underlying risks. Click through 'I agree' privacy policies may be replaced with explicit consent requirements for processing sensitive personal data in the form of consent dashboards, or 'one-time password' (OTP) based consent. Companies will need to be aware of their transfer obligations, including sector-specific data localisation or entering into agreements with transferees having specific provisions as may be approved by the Data Protection Authority. Under the PDP Bill, the monetary penalties for breaching obligations are calculated based on worldwide turnover and can therefore be significant. The PDP Bill may also include a requirement to post details of data security breaches online. Robust data privacy and security measures are expected by all regulators in matters of public procurement, and ISO standards are insisted upon.

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

RANA: Under the IT Act, an individual is entitled to monetary compensation if he or she has suffered any loss attributable to a data breach, however a data processor is not subject to specific penalties for failure to implement adequate security standards and processes. Limited precedents exist for application of the compensatory remedy. This is set to change under the PDP Bill. In addition to compensation for individuals, the PDP Bill envisages specific consequences for data fiduciaries. Depending on the nature of the breach, penalties can extend up to US$2m or 4 percent of the total worldwide turnover of the preceding financial year, whichever is greater. Data fiduciaries can also be penalised around US$80 per day for not allowing individuals to exercise their rights for each day of the default, which is capped at a certain value. They can also be penalised around US$300 for not complying with directions of the Data Protection Authority for each day of the default, capped at a certain value, and around US$150 for each day of the default, capped at a certain value, for not providing the required reports or information.

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

RANA: In August 2017, the Indian Supreme Court delivered a landmark decision declaring the 'right to privacy' as a fundamental right. This has elevated the status of the 'right to privacy'

which can now be interfered with only by a specific law and a procedure which is fair, just and reasonable. After this judgment, except for banks, the private sector's access to biometric information available under the Aadhaar database was struck down. An enablement, however, has now been provided for regulated non-bank entities to use the Aadhar database for authentication purposes, subject to receipt of approvals and compliance with multiple conditions, including those governing security of the underlying data. The PDP Bill embodies similar principles and imposes data privacy obligations on the private sector and the state, while providing the latter with additional exemptions.

Q. In your experience, what steps should a company take to prepare for a potential data security breach, such as developing response plans and understanding notification requirements?

RANA: Companies have the discretion to determine how they prepare for a potential data security breach. The preparation steps, as well as the level of preparedness, varies depending on the size of the business, the nature of the information being processed, the retention period, the purpose of the data retention or processing, transfer requirements and so on. We believe the degree of preparation should be aligned with the possible harm that can be caused in the event of a security breach. An ideal preparation checklist should include a standard operating procedure that identifies possible breach incidents and describes remedial actions as per the severity of the breach, identifying teams and personnel responsible for responding to the breach, investigating the cause, protecting unaffected systems, reviewing existing security safeguards, mandatory and frequent transaction monitoring, updates, and backups. There should also be mandatory security audits and rectification measures implemented by responsible personnel, transition plans and risk mitigation measures, including stop gaps on further processing to prevent additional harm, a description of the nature of security incidents that need external or internal reporting, identification of minimum security standards to be implemented by third parties who receive data, and continuous review of existing security processes to identify risks.

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

RANA: Companies should formulate internal data protection policies that describe restrictions applicable to employees' access to any personal data. Any access to or usage of personal data should be permitted only for trained security professionals on a 'need to know' basis. All company systems should be protected with security measures, including encryption to disable the unauthorised access or monitoring of personal data. An employee authentication process should be implemented to prevent any misuse, and to minimise localised, extended access or storage of personal data, to the extent possible. Employees should also be provided with initial and recurrent training to understand company policies and their data protection obligations, including personal exposure for them in the event of any violation. To exhibit compliance, companies should retain records of these training sessions, and update their content

"Until such time as the definitive law is implemented, voluntary compliance with advanced international standards is preferred by mature and large businesses."

depending on the nature of processing and recent security threats, if any.

Q. Would you say there is a strong culture of data protection developing in India? Are companies proactively implementing appropriate controls and risk management processes?

RANA: The GDPR and judicial precedents have contributed extensively to data privacy awareness among users and businesses in India. This is particularly helpful as even though an extensive data protection framework in the form of the PDP Bill is yet to emerge, data processing and monetisation continues to exist in India and does require some oversight. Until such time as the definitive law is implemented, voluntary compliance with advanced international standards is preferred by mature and large businesses.

www.azbpartners.com

AZB & PARTNERS
ADVOCATES & SOLICITORS

AZB & Partners was founded in 2004 with a clear purpose of providing reliable, practical and full-service advice to clients, across all sectors. The firm brought together the practices of CZB & Partners in Mumbai and Bangalore and Ajay Bahl & Company in Delhi. Having grown steadily since its inception, AZB & Partners now has offices across Mumbai, Delhi, Bangalore and Pune. The firm has an accomplished and driven team of 400-plus lawyers committed to delivering best-in-class legal solutions to help clients achieve their objectives.

APRAJITA RANA
Partner
+91 (0120) 417 9986
aprajita.rana@azbpartners.com

ROHAN BAGAI
Partner
+91 (0120) 417 9999
rohan.bagai@azbpartners.com

AMAN GERA
Senior Associate
+91 (0120) 417 9999
aman.gera@azbpartners.com

China

HARRISON JIA
DeHeng Law Offices
Partner
+86 139 1091 2175
jiahui@dehenglaw.com

Mr Jia Hui practices mainly in the fields of M&A and insurance. He is also the Chairman Assistant of Belt&Road Service Connections, Deputy Secretary of New Energy International Development Federation, Representative of Chief Lawyer Counsel of China Insurance Association and a member of the Legal and Compliance Committee of the China Insurance Asset Management Association. Mr Jia has advised many international companies and Chinese companies on data protection and privacy related issues.

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

JIA: The introduction of the Cyber Security Law of the People's Republic of China (CSL) has enabled a considerable number of companies to deepen their understanding of the duties of confidentiality and data protection. Companies have begun to develop internal training programmes and upgrade their privacy policies. A few companies have also developed or updated safety management systems and operating procedures. However, there are still some challenges around implementation of evolving privacy laws. Firstly, among the companies which have taken cyber security measures, few have introduced data compliance reviews or consulted third-party professionals on data compliance issues. Secondly, in most companies, some employees fail to understand the importance of cyber security, leaving data disorganised and even uploading data to the cloud without conducting a security assessment. Thirdly, there is a shortage of security officers who truly understand the industry, have the ability to manage work and possess the necessary skills.

Q. As companies increase their data processing activities, including handling, storage and transfer, what regulatory, financial and reputational risks do they face in China?

JIA: The main regulations that impact data protection in China are the CSL and the National Standard of the People's Republic of China for Information Security Technology – Personal Data Security Specification. The Cyberspace Administration of China (CAC) has announced the Measures for Security Assessment for Cross-border Transfer of Personal Information, which is currently in draft form and which would specifically regulate cross-border transfers of personal information. While companies increase their data processing activities, they should ensure they remain compliant with all relevant laws. Failure to comply will see companies face both administrative and criminal penalties. For example, many enterprises tend to outsource data processing to overseas data analysis organisations for professional consideration. Article 37 of the CSL requires critical information infrastructure (CII) operators to conduct security assessments where it is necessary to provide such data to overseas parties. Failure to comply with this article may result in fines, suspension of business or even revocation of business licences.

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

JIA: Violation of data protection or privacy laws in China may lead to both administrative and criminal penalties. Under Article 64 of the CSL, in case of a severe violation, an operator or provider in breach of data security may face fines up to RMB 1m, or 10 times the illegal earnings, suspension of a related business, winding up for rectification, the shutdown of any websites and revocation of a business licence. The person directly in charge may face a fine up to RMB 100,000. Furthermore, Article 286(A) of the Criminal Law stipulates that network service providers that fail to fulfil their legal obligations regarding information network security management, as provided in the laws and administrative regulations, and that refuse to rectify this after being ordered by the relevant authorities, thereby causing leakage of users' information, may face imprisonment or criminal detention of no more than three years or surveillance, concurrently or separately with a fine.

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

JIA: In recent years, cases of data breach and infringement of citizens' personal information have occurred from time to time, which has elevated awareness of information security within China. One of the most prominent cases is the Xu Yuyu Case in 2016, where the victim died of sudden cardiac failure after experiencing telecommunications fraud. One of the key points in this case was that the relevant information platform for the national college entrance examination failed to provide effective data security. Xu's death heightened awareness of fraud and had a deep influence on the protection of personal information within China. There have been other cases that have urged companies

to meet their cyber security obligations. In March 2018, a well-known Chinese payment institution, Alipay, was fined RMB 50,000 by a local branch of the People's Bank of China (PBOC) for over-collection and misuse of personal data. The affiliated company Alibaba was fined RMB 180,000 by the PBOC under the Law on the Protection of Consumer Rights and Interests and Criminal Law for breaching the 'minimum necessary rule' on collecting personal financial data and misusing that data. In August 2018, the Shanghai Administration for Market Regulation imposed a fine of RMB 50,000 on Xingyin Information Technology (Shanghai), as the default state of the user privacy setting interface of the company's app, Little Red Book, was set to allow others to add them as friends, which allowed app users to be accessed by strangers. In addition, they were also accused of not adopting technical measures and methods necessary to prevent leakage of personal data.

Q. In your experience, what steps should a company take to prepare for a potential data security breach, such as developing response plans and understanding notification requirements?

JIA: Companies may, in accordance with national laws and their own industry regulations, guidance, and so on, set relevant internal standards based on their specific circumstances. To prepare for a potential data security breach, companies may take proactive measures to implement data compliance, including conducting data audit and classification management of personal information, important data, trade secrets, state secrets and so on, so that the company has a good command of the data involved in its day to day operations. Companies should also strengthen the review of data-related provisions in contracts and adopt contract-based protective measures. Contractual parties should also agree on the rules for the use of data and the liability for data protection breaches, which should be clearly specified.

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

JIA: Companies should establish internal rules to manage the behavioural norms of employees at all levels, with corresponding disciplinary actions, especially for those who may have access to personal information and data. Regarding the company and its personnel, senior executives and the business, technical and information security departments should jointly participate in data risk management. Senior executives should oversee the company's data protection policy, coordinate all the relevant departments and allocate resources around data protection. The duties of each position relating to data security should be clearly specified. Regarding systems and processes, mechanisms for data security management should be established and supported by corresponding internal processes. Different types of data must be classified and managed in accordance with the level of sensitivity.

"Although most companies have adopted risk control measures on a technical level, there are still many loopholes on the systematic and organisational level which must be improved."

Q. Would you say there is a strong culture of data protection developing in China? Are companies proactively implementing appropriate controls and risk management processes?

JIA: In China, most companies have developed a culture of data protection, but many have not attached equal importance to data security risk management as they have to strategy and financial risk management. Therefore, although most companies have adopted risk control measures on a technical level, there are still many loopholes on the systematic and organisational level which must be improved. Legislators are gradually improving data protection regulations across various sectors. The enforcement authorities have also kept an eye on illegal processing of personal data and imposed administrative penalties in various cases.

www.deheng.com

德恒律师事务所
DeHeng Law Offices

DeHeng Law Offices is one of the leading law firms in China providing comprehensive legal services. It was founded in 1993 as China Law Office and was renamed in 1995 as DeHeng Law Offices, reflecting the firm's evolution from an institution of the Ministry of Justice and its rapid emergence as an independent, private law firm with 37 domestic and foreign branch offices and over 2500 legal professionals. The firm's accomplishments have been recognised by Chambers & Partners, Asian Legal Business and China's legal media. DeHeng has received numerous deal awards recognising its achievements in capital markets, M&A and financing.

HARRISON JIA
Partner
+86 139 1091 2175
jiahui@dehenglaw.com

DING LIANG
Partner
+86 135 2166 8628
dingliang@dehenglaw.com

WANG YINAN
Partner
+86 139 1106 2730
wangyinan@dehenglaw.com

Indonesia

BENNY BERNARTO
TNB & Partners in association with Norton Rose Fulbright Australia
Partner
+62 21 2965 1802
benny.bernarto@nortonrosefulbright.com

Benny Bernarto is a corporate and commercial lawyer based in Jakarta at TNB & Partners, an Indonesian law firm associated with Norton Rose Fulbright Australia. He has an extensive corporate practice covering investments, mergers and acquisitions, infrastructure, energy and related project financing, as well as technology and innovation.

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

BERNARTO: Indonesia has yet to enact a single principal data protection law. Rather, elements of data protection rules are spread across various regulations governing individual sectors, such as financial services, health and life sciences, or are included in the Indonesia Electronic Information and Transaction (EIT) law. Highly regulated sectors, such as financial services, have heightened awareness of the role and importance of data protection, as have multinational corporations with businesses based in Indonesia that are very likely subject to, among other things, the European Union's (EU's) General Data Protection Regulation (GDPR), among others. Most Indonesian companies operating at a national level have yet to gain a full understanding of the importance of confidentiality and what data protection entails.

Q. As companies increase their data processing activities, including handling, storage and transfer, what regulatory, financial and reputational risks do they face in Indonesia?

BERNARTO: In Indonesia, companies are faced with uncertainty as to what regulation governs a certain type of information, with whom the information can be shared and what type of protection must be put in place. In addition to reputational damage, which could take companies years to recover from, financial risks stemming from data breaches include fines of up to approximately US$600,000 and the obligation to compensate affected customers. The Indonesian electronic information and transactions (EIT) law sets forth sanctions including warning letters, the suspension of business and imprisonment.

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

BERNARTO: Although Indonesia's data protection law is yet to be finalised, the EIT law guarantees a person's right to claim damages arising from a breach or violation of their data. In the financial sector, the maximum penalty is approximately US$600,000 and the minimum penalty is approximately US$300,000. As elements of data protection rules are spread across various regulations governing sectors such as financial services, health and life sciences, other types of sanctions are also imposed by the relevant regulations in these sectors.

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

BERNARTO: One of the most recent data breaches involved two subsidiaries of an Indonesian airline, Lion Air Group, which saw millions of customers' personal details leaked online. The airline issued a statement saying that all its systems are fully secured and none of the payment details of customers were compromised. This has put a spotlight on data protection, which is a concern among businesses in Indonesia, as it highlights the fragility of data security and the impact it has on data owners. Indonesia has a growing digital economy and with the advancement of technology comes the

exchange of great amounts of data. The draft regulation on personal data protection seeks to regulate the importance of consent in sharing or transferring a person's personal data to prevent, among other factors, the buying and selling of personal data.

Q. In your experience, what steps should a company take to prepare for a potential data security breach, such as developing response plans and understanding notification requirements?

BERNARTO: In addition to having secure data infrastructure, companies should regularly educate employees on how to prevent data security breaches. This could be done through training and refresher courses and internal guidance, as well as through establishing standard operating procedures (SOPs) governing how the company should act in the wake of an incident. Due to its regulatory exposure, some multinational corporations conduct regular simulations of data breach incidents to test and spot flaws in their SOPs, especially related to its system, cross-department containment measures and crisis situation line of command structure, which also relates to accountability.

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

BERNARTO: In educating employees on measures to prevent data breaches, incident SOPs and consequences for employees proven to have compromised proprietary data, companies could also ensure employees are clear about the applicable regulation related to whistleblowing. Applying a tiered information access system could help manage the risk of a data breach in some organisations. In engaging external vendors, particularly those involved in data processing or which have access to a company's data due to the products or services they provide, the company's designated data protection officer could impose and monitor a set requirements that vendors must adhere to, to ensure that the company's data is not shared with unauthorised parties.

"In addition to having secure data infrastructure, companies should regularly educate employees on how to prevent data security breaches."

Q. Would you say there is a strong culture of data protection developing in Indonesia? Are companies proactively implementing appropriate controls and risk management processes?

BERNARTO: Indonesia is developing a strong culture of data protection. Factors that are influencing this mindset include the country's growing digital economy, the financial technology (FinTech) sector, and the advancement of technology across all lines of business. Although the overarching data protection bill is still being deliberated across governmental and parliamentary levels, there are regulations in place which govern certain business sectors and aspects of data protection. This, in addition to regulations such as the GDPR, have prompted companies operating in Indonesia to implement risk management processes. However, companies in Indonesia that have yet to see the direct impact of data protection requirements on their operations might be taking a slower road to compliance.

www.nortonrosefulbright.com/id

TNB & PARTNERS
In association with Norton Rose Fulbright Australia

TNB & Partners works in association with Norton Rose Fulbright Australia, advising multinational and local entities across key industry sectors in corporate and commercial, banking and finance, as well as dispute resolution practices.

RIZKY RADITYA LUMEMPOUW
Associate
+62 21 2965 1815
rizky.lumempouw@nortonrosefulbright.com

Israel

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

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

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

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

Q. As companies increase their data processing activities, including handling, storage and transfer, what regulatory, financial and reputational risks do they face in Israel?

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

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

RAVIA: Administrative fines of up to approximately US$6500 are imposable under Israeli law for violations of the Israeli privacy law's data protection regime. Continuous violations following a cease and desist letter can increase the fine by an additional 10 percent for each day during which the violation continues. Finally, most forms of invasion of privacy under the law's privacy regime can also give rise to a criminal offence punishable by up to five years in prison. However, under the current regime in Israel, no regulatory fines are imposable in cases of data breaches resulting from an organisation's failure to implement the data security safeguards required under the Israeli data security regulations, and regulatory enforcement powers are quite limited. Attempting to resolve this, the Israeli privacy regulator sought to advance an amendment to the law that would grant the regulator greater and more expansive

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

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

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

Q. In your experience, what steps should a company take to prepare for a potential data security breach, such as developing response plans and understanding notification requirements?

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

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

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

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

Q. Would you say there is a strong culture of data protection developing in Israel? Are companies proactively implementing appropriate controls and risk management processes?

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

www.pearlcohen.com

PEARL COHEN

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

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

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

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

FW
ANNUAL REVIEW

www.financierworldwide.com