Market
Intelligence

PRIVACY & CYBERSECURITY 2022

Global interview panel led by WilmerHale

LEXOLOGY
Getting the Deal Through

LEXOLOGY
Getting the Deal Through

Publisher
Edward Costelloe
edward.costelloe@lbresearch.com

Subscriptions
Matthew Bridgewater
matthew.bridgewater@lbresearch.com

Head of business development
Adam Sargent
adam.sargent@gettingthedealthrough.com

Business development manager
Dan Brennan
dan.brennan@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

Cover photo: shutterstock.com/spaintervfx

ISBN:978-1-83862-999-1

Printed and distributed by Encompass Print Solutions

PRIVACY & CYBERSECURITY 2022

and the PIPL.

Global Trends

Jason Chipman is a WilmerHale partner who advises companies on complex regulatory matters associated with data security, cyber incident response, the Committee on Foreign Investment in the United States and related export controls. He has assisted companies in most sectors of the economy on data security best practices and frequently assists with corporate due diligence. Mr Chipman currently serves as a non-resident fellow at the National Security Institute.

Benjamin Powell is a WilmerHale partner who has advised companies on major cybersecurity incidents and preparedness across virtually every sector, including banking, investment management, retail, defence and intelligence. He is recognised as a leading attorney in international investment and mergers, including the Committee on Foreign Investment and the Defense Security Service.

Arianna Evers is a WilmerHale special counsel who advises clients on complex privacy, data security and consumer protection issues arising under rapidly evolving federal and state requirements. She regularly assists clients on privacy-related issues, including legal requirements and best practices in emerging and changing areas of the law, and also represents them in regulatory investigations.

Shannon Togawa Mercer is a WilmerHale senior associate who advises clients on matters related to cybersecurity, privacy, and US and European data protection. She joined WilmerHale from the London location of a large global law firm where her practice focused on transactional work, including the cybersecurity and data protection aspects of capital markets transactions and mergers and acquisitions.

Cybersecurity continues to represent a growing risk for companies around the world with cyberthreats posed by nation states, commercial competitors, company insiders, transnational organised crime and 'hacktivists' continuing to grow on a global basis. The covid-19 pandemic has made this trend particularly acute as businesses around the globe work to navigate a more distributed work force and, potentially, more vectors for cyberattacks. Prominent ransomware attacks have also raised new worries about destructive cybersecurity events that have an immediate impact on affected businesses. The ongoing conflict in Ukraine has also increased concern about cyber risk.

In this environment, maintaining an effective corporate cybersecurity programme is the standard expectation for all businesses. The ability to respond efficiently and effectively to data security emergencies will be important for avoiding potentially disruptive cybersecurity incidents in the future and for navigating related regulatory actions. In the United States, enforcement authorities are devoting growing resources to countering cyberthreats. For example, the Office of Financial Assets Controls (OFAC) issued an October 2020 directive providing guidance specifically addressing ransomware events, warning potential victims that ransom payments could violate US sanctions laws and regulations and in September 2021 issued an updated advisory. OFAC has also begun to enforce sanctions against cryptocurrency exchanges that facilitate ransomware payments. Governments in Europe, Asia and North America have been responding to these trends as well, with particular focus on privacy and security controls for companies possessing large amounts of personal information.

Jurisdictions around the world continue to refine regulatory requirements for businesses identified as possessing important data. In the United States, while data security continues to be handled through sector-specific regulations and through state laws, there is a growing push to create privacy legislation potentially similar in scope to the EU General Data Protection Regulation (GDPR). Many states in the United States are exploring the creation of new privacy rules that would include basic data safeguarding requirements, and California, Colorado, Virginia, Utah and Connecticut have all enacted laws requiring new privacy controls. State attorneys general continue to devote substantial resources to policing private sector data breach notification compliance.

At the federal level, data security regulatory requirements are most onerous for specific economic sectors believed to possess higher risk data, such as federal government defence contractors, banks and healthcare companies. For example, on 15 March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 was signed into law, creating new reporting requirements for critical infrastructure entities. Previously, on 12 May 2021, President Joe Biden issued


Jason Chipman


Benjamin Powell


Arianna Evers


Shannon Togawa Mercer

an executive order focused on combating threats to US computer systems. The Executive Order on Improving the Nation's Cybersecurity (Cybersecurity EO) sets out to improve cybersecurity, particularly in relation to federal government systems, and follows several high-profile cyber incidents in 2020 and 2021. President Biden also issued an executive order mandating the US federal government to create new cybersecurity standards for all contractors. The Office of Management and Budget (OMB) released software supply chain security guidance under the Cybersecurity EO directed at federal agencies and in May 2022, the National Institute of Standards and Technology (NIST) provided guidance on supply chain cyber risk for organisations. While many standards promulgated in 2021 relate to federal agency security, companies operating in the United States face a patchwork of state and federal regulatory guidelines and requirements that may impact their data security obligations with trends moving toward increased oversight and, potentially, a comprehensive federal data protection law for data security controls.

In Europe, the regulatory environment remains fluid. In June 2021, the European Commission published new standard contractual clauses (SCCs) for cross-border data transfers. These are the first new SCCs in more than a decade. Companies and regulators are still navigating the landmark Court of Justice of the European Union ruling invalidating the EU–US Privacy Shield framework, while eagerly awaiting the results of negotiations concerning its successor. At the same time, companies in the European Union continue to grapple with compliance with the 2018 Network and Information Security (NIS) Directive and the GDPR, both of which introduced major data security regulatory changes for certain companies operating in the EU and triggered a wave of corporate activity to update privacy policies and put in place appropriate compliance controls. Enforcement actions have been growing over the past few years. European regulators imposed over US$1 billion in fines in 2021 (as opposed to around US$180 million in 2020). Furthermore, on 1 January 2021, the UK formally left the EU (Brexit), and has formed a UK-specific data protection regime (the UK Data Protection Action 2018 and the UK GDPR), including new contractual terms to safeguard data transfers out of the UK.

In China, the Personal Information Protection Law (PIPL) became effective on 1 November 2021. The law includes parameters within which cross-border data transfers of personal information may be made for business and other reasons, including where consent or a security assessment may be required to effectuate the transfer. Violations of the PIPL could lead to fines ranging between US$150,000 (or US$1,500 to US$15,000 fines on directly responsible supervisors or individuals) or in serious cases, US$7.7 million or up to 5 per cent of a company's previous year's business revenue. Furthermore, it is possible that for particularly serious instances of non-compliance, companies or their employees, or both, might be criminally

liable. Notably, the PIPL applies not only to personal processing activities within China, but also to processing outside China of personal information of individuals who are inside China when the processing is for the purpose of providing products or services to individuals inside China, analysing or evaluating the behaviour of individuals inside China or for other circumstances prescribed by law or regulation. In 2021, China also published draft regulations on the Administration of Network Data Security providing detail to implement the Chinese Cybersecurity Law, Data Security Law and the PIPL.

Other Asian as well as African countries have also been actively legislating data protection and privacy, with Thailand, Sri Lanka, Uganda and South Africa all passing comprehensive laws and Japan and South Korea amending their established privacy laws.

It appears likely that data security requirements will continue to expand globally in the near term. For international companies, changing and expanding cybersecurity standards will continue to complicate company network security operations with special handling rules applying to the hosting and processing of sensitive data, such as personal data about consumers, critical infrastructure data and financial sector data. Cybersecurity will remain a major issue for these organisations and will continue to require technical, legal and communications experts to work together to manage the risk of data security incidents.

Jason Chipman
jason.chipman@wilmerhale.com

Benjamin Powell
benjamin.powell@wilmerhale.com

Arianna Evers
arianna.evers@wilmerhale.com

Shannon Togawa Mercer
shannon.mercer@wilmerhale.com

Wilmerhale
Washington, DC
www.wilmerhale.com

Armenia

Narine Beglaryan is an attorney who joined the Concern-Dialog law firm in September 2013 as senior associate. Since 2016, she has been a partner of the firm.

Narine specialises in banking law, corporate law (she heads the corporate law and banking law and compliance areas of practice of the firm), contract law and in-court representation of her clients' interests in administrative and civil cases. At present, she specialises in the sphere of anti-money laundering and combating the financing of terrorism and data protection.

In the sphere of law, she started her practical activity in 2007. Prior to joining our team, Narine had worked with Armentel CJSC (now Team Telecom Armenia) as a legal adviser at the Department of Legal Support to the Business. For many years, she had been employed at the legal office of BTA Bank CJSC in the position of chief lawyer of the Legal Office.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

By decision No 183-L of 11 February 2021, the Armenian government approved the Digitalisation Strategy of Armenia, as well as the Action Plan of the Digitalisation Strategy of Armenia and its performance indicators.

The Strategy was developed by the Ministry of HighTech Industry of the Republic of Armenia, which is the main department responsible for the implementation of the strategy.

As the main objective, the Strategy envisages the digital transformation (digitalisation) of the government, economy and society of Armenia. Among the means to achieve this goal, the introduction and development of a cybersecurity system in the country was highlighted.

As a first step in the implementation of the cybersecurity system, it is envisaged that the Ministry of HighTech Industry will develop a comprehensive overall cybersecurity policy and action plan. At the moment, such a document is not available on public discussion platforms (for example, on the e-draft.am website) and the platforms of normative legal acts that have entered into force (for example, arlis.am).

The same strategy provided for the establishment of a Cybersecurity Centre of Excellence, which should develop cybersecurity standards (it is proposed to take the experience of the US, the UK and Israel as a basis and localise international cybersecurity standards).

The Action Plan of the Strategy provides that the Cybersecurity Centre of Excellence, after the start of its activities, will check the compliance of state platforms with the developed standards, periodically conduct review of cybersecurity standards and approve standards, check the application of standards, and certify systems, provide expert advice, monitor the level/condition of cybersecurity, develop guidelines for cybersecurity literacy enhancement and knowledge development and provide incubation programmes, conduct artificial intelligence research projects, support and promote start-ups in the field of cybersecurity. According to the information currently available, the Cybersecurity Centre of Excellence has not been established yet.

The government has also determined the classification of the risks associated with cybersecurity, the development of an additional cybersecurity enhancement plan and relevant scenarios in order to strengthen cybersecurity in the event of emergencies, war, the establishment of exercises related to certain incidents and measures and principles aimed at coordinated accident management (at the moment these are also not adopted).


Narine Beglaryan

It is important to note that for the effective implementation of programmes related to cybersecurity, the need for the formation and development of cybersecurity literacy is highlighted, and the implementation of measures and programmes in this direction is envisaged.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The regulation of unlawful operations performed upon personal data in Armenian normative legal Acts may be found exclusively in the main Act regulating the sphere, which is the Armenian Law on Personal Data Protection.

The obligation to take measures against unlawful operations performed upon personal data is provided by the Armenian Law on Personal Data Protection exclusively for the controller.

When unlawful operations performed upon personal data are revealed that at the same time do not qualify as outflow of personal data from electronic systems,

the controller shall be obliged to eliminate the committed violations. If the controller cannot eliminate the violations committed within three working days, or it is initially obvious that it is impossible to eliminate the violations, the controller shall be obliged to immediately destroy the personal data. When the controller eliminates the violation or destroys personal data, the controller shall inform the data subject or his or her representative about it. If a violation was discovered based on a request from the Agency for Protection of Personal Data of Armenia, the controller must also notify the Agency for Protection of Personal Data of Armenia. Notification to both the data subject (representative) and the Agency for Protection of Personal Data of Armenia shall be sent within the three working days after the elimination of the violation or destruction of personal data.

In the event of outflow of personal data from electronic systems, the controller must immediately publish an announcement about the incident. In parallel with the publication of the announcement, the controller shall officially report on the outflow the Police of the Republic of Armenia, as well as the Agency for Protection of Personal Data of Armenia.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

The requirements for security measures during the processing of personal data are set out in the Armenian Law on Personal Data Protection. The Armenian Law on Personal Data Protection requires the controller to use encryption keys. This security measure should protect personal data, particularly: the protection of information systems containing personal data against accidental loss, unauthorised access to information systems, unlawful use, recording, destroying, altering, blocking, copying, disseminating personal data and other interference.

The list of security measures also includes the controller's obligation to prevent persons without the right from processing personal data. The controller should also restrict access and use of technologies and data to permitted purposes and lawful use.

In the context of security, in the case of data transfer to the processor by the controller, the agreement with the processor must specify technical and organisational measures for the protection of personal data that the processor will be obliged to comply with when processing personal data transmitted by the controller.

With the exception of certain industry organisations (specifics are discussed in the following question 6), there is no requirement for controllers or processors to obtain a certificate of compliance with the requirements of international standards and the requirements of relevant standards applied in the field of information security.

> "Liability is currently applied to a natural person who, in the event of an administrative offence, is the director of a legal person considered as a processor or controller of personal data."

In Armenia, the legal consequences of violations of personal data processing security requirements arise in the form of administrative or criminal sanctions. In both cases, liability is currently applied to a natural person who, in the event of an administrative offence, is the director of a legal person considered as a processor or controller of personal data, and in the event of a crime – the persons who committed the crime.

Administrative responsibility for security arises for non-use of encryption keys, and the fine is about US$200. Another security- related administrative offence is the violation of the requirements for ensuring the security of personal data processing in information systems, where the fine amounts to between US$200 and US$400. These violations are considered an administrative violation if they do not constitute a crime.

Personal data subjects cannot claim moral (intangible) damages for violations committed by controllers or processors when processing their data, but they must be able to prove material damage (actual damage or lost benefit, or both), which is rather complicated as regards to the feasibility of proving it.

In general, considering the security requirements and the consequences of their violation, it turns out that for violations of the security requirements for processing personal data, the risk to the controller and processor is not directly financial, but rather reputational, such as possible business losses after gaining a reputation for not ensuring the security for processing of personal data.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

In Armenia, the most regulated sphere in terms of information security is the financial and banking sphere. Here, since 2014 in accordance with the procedure on establishing minimum requirements for ensuring information security approved by the Board of Central Bank of the Republic of Armenia, priorities, and compliance requirements for information security of financial and banking organisations have been determined.

The information security management system for banks operating in the territory of Armenia – regulatory market operator, central depository, credit bureaus,

Photo: shutterstock.com/Leonid Andronov

leveraged transactions, including persons providing investment and non-core services related to Forex transactions and crowdfunding platform operators, as well as insurance companies and payment and settlement organisations – has been brought into compliance with the requirements of international standards applied in the field of information security. At the same time, regardless of compliance, these organisations are obliged to ensure continuous satisfaction of the requirements established by the procedure on establishing minimum requirements for ensuring information security, approved by the board of Central Bank. As a result of these measures, the financial and banking organisations listed here are mostly protected.

As mentioned in question 5, the main rules of the security of personal data are mostly generic and at the same time, organisations are not required to comply with international standards and confirm this compliance with a certificate. This leads to the fact that a significant part of organisations (especially small and medium-sized businesses) do not take technical security measures or do not take sufficient measures.

It is also important to note that the requirements of the security of personal data processing imposed by an organisation by its internal acts differ depending on the composition of the company's participants: that is, organisations with foreign investments (mainly European countries and the US) have technical security measures and requirements adopted, unlike other organisations. Information security measures are highlighted in certain industry companies (electronic communication service providers).

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

The use of the original cloud technologies in the processing of personal data is not prohibited as such; therefore, it can be carried out in compliance with the general rules.

However, during the transfer or transmission of personal data to the cloud hosting environment, several issues requiring solving have arisen before the organisations.

First, when transferring personal data to the cloud hosting environment, the organisation should find out whether personal data is transferred to a third party and whether personal data is transferred to another country or not.

As a rule, the transfer of personal data to the cloud hosting environment is a transfer to a third party, unless, of course, the organisation uses its own servers. Here, the organisation must make sure that the consent of the personal data subject has been obtained for the transfer of data to a third party.

Also, as a rule, the transfer of personal data to the cloud hosting environment involves the transfer of personal data to the territory of another country, since usually the servers are physically located in the territory of another country outside of Armenia. The approach is that if the server, technologies or data processing centres are physically located outside Armenia, the organisation transfers personal data to another country. The organisation must make sure before transferring personal data that it has received the consent of the personal data subject and must check.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The Investigative Committee has a Department of Investigation of Cybercrime and High Technology Crime. This department of a law enforcement body is authorised to investigate of crimes against the security of computer information.

The Criminal Code of Armenia in force defines seven main crimes against computer information security (articles 251–257). These are: (i) access (penetration) into computer information systems without permission; {ii) change in computer information; (iii) computer sabotage; (iv) illegal appropriation of computer data; (v) manufacture or sale of special devices for illegal penetration into a computer system or network; (vi) manufacture, use and dissemination of hazardous software; and (vii) breach of rules for operation of a computer system or network.

The new Criminal Code of Armenia will enter into force on 1 July 2022. Again, seven crimes against the security of a computer system and computer data have been established (articles 359–365): (i) penetration into a computer, computer system or computer network; (ii) change in computer data; (iii) computer sabotage (smuggling); (iv) illegal seizure of computer data or their appropriation; (v) illegal circulation of special software or tools; (vi) fraud; and (vii) violation of the rules or requirements for the operation of a computer, computer system or network. One of the main changes is that the list of technologies, solutions and tools with which or by which computer crimes can be committed has been expanded and clarified to some extent.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

In most transactions, clients do not require due diligence prior to M&A deals or in M&A deal negotiations and the conclusion of transactions and do not plan to check issues related to personal data protection.

"The main rules of the security of personal data are mostly generic and at the same time, organisations are not required to comply with international standards and confirm this compliance with a certificate."

When considering personal data and their security issues for M&A deals themselves, the compliance with the Law on Personal Data Protection should be verified. It is necessary to pay attention to the actual situation of data processing by the organisation, including the consent of the subjects of personal data, the purpose of processing, the scope of data transmission and the provision of access to data. Then, it is necessary to compare the factual situation with the provisions of the law and to find out the inconsistencies. The main risks concern the legality of processing and proportionality; thus there may be incomplete consents or non-purpose uses.
We believe that during M&A deals it is important to pay attention to, and to exclude, the sale of personal data during the transaction. Personal data is not an asset of a company. If as a result of the acquisition of a company or company's assets the circle of persons with access to the data will be changed, ensure that the consent of the personal data subjects is obtained

Narine Beglaryan
narine.beglaryan@dialog.am

Concern Dialog CJSC
Yerevan
www.dialog.am

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

It is necessary to choose a lawyer with an understanding of the specifics of information technology. It is important that a lawyer can fully visualise and understand business process in order to be able to offer practical solutions or assess practical risks. At the same time, as a personal data lawyer, it is preferable to have at least a general knowledge of other countries' approaches and acts in the field of personal data protection.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

Advising on cybersecurity and privacy is sometimes complex due to the lack of regulation. The privacy regulations are in place; however, most concepts were adopted in 2015, and since then no major changes took place. Regulation is generic, for example, in comparison with the GDPR rules; on the one hand this is positive thing because it allows the avoiding of bureaucracy and more flexibility, but on the other it sometimes leads to an absence or lack in data security, which may cause leakage.

How is the privacy landscape changing in your jurisdiction?

After the adoption in 2015 of the Law on Personal Data Protection and the creation of the Agency for the Protection of Personal Data, special attention is paid to the issue of personal data protection in the country. Cybersecurity issues became more relevant and problematic because of the hacking by Azerbaijan during the 44-day Artsakh War in 2020.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

The dangers of cybersecurity incidents in Armenia are similar to the dangers in other countries. In general, organisations should be able to implement information security systems, which will include both the use of technological means and the availability of internal procedures. As with any system, human resource management requires efficiency.

China

Jingyuan Shi is a partner in the Shenzhen office of Simmons & Simmons, and is responsible for the TMT practice in the Greater China region. She is a PRC-qualified lawyer and a practising solicitor in England and Wales.

She focuses her practice on the telecoms, media, and technology (TMT) sector. She has in-depth knowledge of the TMT industry from various perspectives, primarily advising on all sorts of corporate and commercial transactions, data compliance issues and general regulatory matters. She is experienced in cross-border work, start-up financing, regulatory compliance (including competition work) and intellectual property matters. Jingyuan is regularly invited to speak at industrial events and contributed to the China chapters of *Lexology Getting The Deal Through – Fintech* (2017–2021) and *Lexology Getting The Deal Through – Telecoms & Media* (2017–2021). Jingyuan holds an LLB from Fudan University and an LLM (IP and IT law) from the London School of Economics and Political Science (Distinction).

Yuchen Lai is a PRC qualified lawyer based at Simmons & Simmons' Shenzhen office.

Yuchen works extensively for international and Chinese TMT companies, investors, financial institutions, asset managers, fintech companies and life sciences companies. She advises on a wide range of compliance issues and has a strong focus on data advice and has in-depth knowledge and rich experience in Chinese and global data compliance projects.

Previously, Yuchen was a senior journalist with a large media organisation in China, focusing on legal reporting. She excels at regulation and policy analysis and providing comprehensive, pragmatic and commercial advice. She holds a BA from Sun Yat-sen University and an MSc from the London School of Economics.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

There have been significant developments in China regarding cybersecurity, protection of personal data and privacy in general in recent years. China, for the purpose of this chapter only, refers to mainland China, without taking into account the laws and practice in Hong Kong SAR, Macau SAR and the Taiwan region.

The Civil Code took effect on 1 January 2021, which sets the fundamental principles for protection of personal data and privacy. The triangulated safeguard for data regulation, namely the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law (PIPL), are ready in position to set the key regulatory framework in China. The Cybersecurity Law took effect in 2017; the Data Security Law took effect on 1 September 2021; and the PIPL took effect on 1 November 2021.

The Cybersecurity Law is the first legislation in China to comprehensively regulate the country's cyber networks. It applies to the construction, operation, maintenance and use of networks, as well as to cybersecurity supervision and management within the territory of China. The Cybersecurity Law is wide in scope, containing an overarching framework targeting the regulation of network security, protection of personal data, and safeguards for national cyberspace sovereignty and security. It is the foundation of other laws, regulations and industrial rules related to cybersecurity and personal data protection. It relates more to data in general rather than focusing on personal data (although there are certain provisions in relation to personal data).

The Data Security Law is the first fundamental law on data security in China. It relates more to data in general rather than focusing on personal data. It sets out the overall principles and structure of China's data security legal regime from a national security and sovereignty point of view. A key concept under this new law is the categorised and hierarchical data protection system. The specific scope and catalogues of 'important data' are required by this law to be formulated and published by regional and sectoral regulators. Cross-border transfer of such 'important data' is subject to specific requirements. Given 'important data' is a key concept used at various places during this chapter, before the aforesaid catalogues are published and for reference purposes at this moment, in one of the draft guidelines (not effective and not mandatory), 'important data' is defined as data collected and generated by organisations and individuals within China that is not a state secret but closely relevant to national security, economic development or public interest.

The PIPL is the first comprehensive law on personal data protection in China. It establishes rules for personal data processing, the protection of sensitive personal data, cross-border transfer, rights of personal data subjects, and obligations of

personal data processors and their entrusted parties when processing personal data. The PIPL borrows many key concepts from the EU General Data Protection Regulation (GDPR), such as extraterritorial effect on overseas processing of personal data of China-based individuals for the purpose of offering products or services to, or for analysing and assessing the behaviour of, such individuals; more legal bases for the processing of personal data, in addition to consent, which used to be the only lawful basis under Chinese law; the concept of data protection impact assessment but with lower triggering thresholds than GDPR. Meanwhile, the PIPL maintains an equal amount of unique features to reflect local regulatory and business needs; for example, legitimate interest is not included as one of the legal bases for processing personal data; it proposes restrictions on the cross-border transfer of personal data by the nature of the transferors.

One key accompanying regulation to the three laws mentioned above is the Regulation on Security Protection of Critical Information Infrastructure that took effect on 1 September 2021. It clarifies the scope of Critical Information Infrastructure (CII) and provides that regulators of key sectors (eg telecoms, energy, transportation, finance, defence, etc) are responsible for formulating CII

identification rules and identifying CIIs. The regulation stipulates obligations for CII operators, including, among others, conducting cybersecurity monitoring, test and risk assessment, formulating and implementing contingency plans, establishing security protection policies for personal information and data; reporting cybersecurity incidents and important matters, and completing cybersecurity review under certain circumstances (see below). Each CII operator must appoint a specialised body to take care of the cybersecurity issues, and key members of this body must go through security background checks.

Another noticeable regulatory update is the amended Cybersecurity Review Rule (which took effect on 15 February 2022), and this amendment was jointly published by the Cyberspace Administration of China (CAC) and 12 other government departments on 28 December 2021. The concept of security review was firstly introduced in the Cybersecurity Law, which requires CII operators to apply for national security review on their procurement of network product and services if it may impact national security. The amended Cybersecurity Review Rule extends the cybersecurity review to data processing activities that impact or may impact national security, by internet platform operators. In particular, an internet platform operator must apply for cybersecurity review over its proposed listing outside of China, if it possesses over one million users' personal data. This will have a severe impact on data-rich technology companies seeking a listing in a foreign country. The substantial parameters for such review are, among others, to verify whether there are risks of theft, leakage, damage or illegal cross-border transfer on 'core data', 'important data' or a large volume of personal data, and following the listing in a foreign country, whether the CII, 'core data', 'important data' or large volume of personal data might be influenced, controlled or maliciously used by a foreign government. 'Core data' is defined under the Data Security Law as such data that relates to national security, lifelines of the national economy, people's livelihood or major public interest. The amendment proposes to extend the statutory review period from 45 working days to three months or even longer.

In addition to mandatory laws and regulations, the Personal Information Security Specification (GB/T 35273-2020), which took effect on 1 October 2020, is a recommendatory national standard. This is a comprehensive and practical guideline for data compliance. Compared with the 2017 version, it has made many significant changes. It adds restrictions on user profiling (eg, user profiling should not have contents regarding race, religion, disability or disease discrimination); it makes specified requirements for personalised display (eg, during e-commerce service, any personalised display of products or services based on the consumer's interest or preference or consumption habits shall be accompanied by options that are not personalised); it adds requirements for third-party access management (eg, built-in

> “When hit with a data security incident, companies must be able to multitask on many pressing issues at the same time.”

security risk assessment mechanism in advance, identification of such third-party access to consumers); it sets rules for appointing data protection officers or similar positions based on the size of the company or volume of user information they process; and it establishes specific rules and guidelines on handling sensitive personal data, including storage, sharing, transfer, public disclosure and incident notice.

On 29 October 2021, CAC published the Draft Measures for Data Export Security Assessments (Draft Security Assessment Measures) for public comments. The Draft Security Assessment Measures set out the procedures, required materials and criteria for security assessments for cross-border data transfer. This draft proposes to expand the applicability scope of security assessment required under the Cybersecurity Law, Data Security Law and the PIPL.

On 14 November 2021, CAC released the Draft Administrative Regulation on Network Data Security (Draft Regulation) for public comments. The Draft Regulation sets out various rules regarding the processing of ‘important data’ and personal data. It has a wide range of extraterritorial applicability, which includes processing data of China-based individuals and organisations: (i) for the purpose of

offering products or services in China; (ii) analysing or assessing the behaviour of China-based individuals and organisations; or (iii) processing 'important data'. The Draft Regulation expands the extraterritorial effect of the PIPL to those processing activities targeting both China-based individuals and organisations.

On 10 February 2022, the Ministry of Industry and Information Technology (MIIT) released the updated Draft Administrative Measures for Data Security in the Areas of Industry and Informatization (the MIIT Draft Regulation) for public comments. This MIIT Draft Regulation applies to the processing of industrial, telecoms and radio data performed within China.

On 16 March 2022, the Standardization Administration of China (SAC) completed another updated draft of the Rules for Identification of Important Data and published it for public comments. According to this latest draft, the definition of 'important data' is revised as 'data in specific areas, groups, regions, or data reaching certain accuracy or scale, once leaked, tampered with or damaged, may directly endanger national security, economic operation, social stability, public health and safety'. The designation of 'important data' shall be consequence (rather than data type) driven.

Photo: shutterstock.com/Eric007

In addition, regional legislators are also actively formulating data-related regulations. As of the date of our response, regional data regulations of Shenzhen Special Economic Zone (effective on 1 January 2022), Shanghai City (effective on 1 January 2022) and Chongqing City (effective as from 1 July 2022) have been published.

From the law enforcement side, the statistics on the official website of the CAC shows that the CAC, together with other relevant government departments, has closed down more than 33,000 applications; blocked more than 2.34 million website links; and frozen more than 3.64 million illegal user accounts, involved in pornographic, gambling, malware or illegal gaming activities. The CAC launched special campaigns for eight months in 2020 to regulate online activities in China.

In particular, the CAC, the MIIT, the State Administration of Market Regulation and the Ministry of Public Security together launched a campaign against illegal collection and processing of personal data via mobile applications that has been running since late 2019. According to statistics published in June 2022, the MIIT has examined over 3.22 million mobile applications in the market, and ordered nearly 3,000 applications to rectify their non-compliant processing activities or suspend services.

In addition to the crackdown on low-profile illegal activities, the CAC also targets some of the high-profile leading players in the market. For example, in early July 2021, the CAC initiated cybersecurity review investigations against several leading transportation and logistics applications in China. The CAC and its local counterparts have continued with various law enforcement campaigns to target violations such as internet violence lately.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The Cybersecurity Law requires network operators to notify competent regulators of cybersecurity incidents including personal data breaches, but it does not go on to provide details about the key factors to be assessed. A set of lower-level regulations and standards provide guidelines in this regard. The reportable incidents usually include cyberattacks, hacking, malware, virus and human or equipment failure that may cause significant damage to the society and general public. Subject to the affected areas and degree of damage, there are different categories of reportable breaches. The key factors or impact of an incident that an organisation must assess include: (i) internet access in geographic areas (eg, single or multiple provinces, or even the entire country); (ii) operation of major websites or platforms (eg,

e-commerce websites with millions of active users); (iii) number of users affected (a minimum of 100,000 users should ring alarm bells); (iv) loss, theft or falsification of state secrets, important or core data that may cause significant damages; and (v) a catch-all scenario applicable to other factors, judged by the discretion of the organisation suffering the breach incident.

Upon initial assessment, if an organisation believes any of the above factors is met, it should immediately report such breaches to regulators. If a breach incident is likely to cause severe harm to the lawful rights and interests of individuals (eg, where sensitive personal data is leaked), the organisation shall inform the affected individuals of such breach incident.

The PIPL requires the processors of personal data (note the definition of personal data processor under Chinese law is essentially equivalent to the concept of a personal data controller under the GDPR) to notify the competent regulator and relevant individuals once a personal data breach is detected. If the processor can take measures to effectively avoid the damage caused by data breaches, then it may decide not to notify the affected individuals. However, if the data protection regulators find the breaches may cause damage to individuals, they can request the processor to notify the affected individuals regardless. There is so far no general hard time requirement on when such report must be done under the PIPL, but we recommend data processors to report as soon as possible if initial assessments point to a report.

In addition, note that there are likely sectorial rules with more specific timing requests on this issue. For example, for financial institutions, according to the Implementation Measures for Protecting Financial Consumers' Rights and Interests, which took effect on 1 November 2020, reports to consumers and the regulators must be made within 72 hours. The Measure for Supervising the Risks of Information Technology Outsourcing Activities by Banking and Insurance Institutions, which took effect on 30 December 2021, provides that banks shall report to China Banking and Insurance Regulatory Commission or its local counterparts within 24 hours of any client personal information breach or data damage/loss during the IT outsourcing activities. The Measures on Reporting, Investigation and Handling of Cybersecurity Incidents for Securities and Futures Sector, which took effect on 4 June 2021, provide that securities and futures institutions must report cybersecurity incidents immediately, and in the event of a severe incident the report shall be updated every 30 minutes. So, in addition to general reporting obligations, an organisation shall closely monitor and follow industry-specific regulations in order to comply with reporting obligations.

> "The amended Cybersecurity Review Rule extends the cybersecurity review to data processing activities that impact or may impact national security, by internet platform operators."

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

When hit with a data security incident, companies must be able to multitask on many pressing issues at the same time. The biggest issues include, but are not limited to, assessment of severity and scope of damage; determination of whether to report the incident to regulators and affected individuals; technical rectification measures to control the incident to minimise damage; complete and swift internal review and investigation of the breach; coordination with outside legal, forensic, technical or public relations counsel to prepare for subsequent actions; cooperation with directives from regulators and the police (if necessary); responses to customer inquiries or complaints; and responses to media reports or coverage.

Any of these issues, if not handled properly, may easily morph into a situation that is out of control, especially in today's social media age. Such an incident is the true test of a company's response strategies, internal policies, management structure, designated staff as well as technical capabilities. The ultimate goal is to

manage potential liabilities on all fronts, manage potential reputational damages, resume normal operation and prevent recurrence of similar incidents.

That said, out of these pressing issues, from a privacy protection perspective companies must concentrate resources to assess damages that may be caused to the privacy of affected individuals and take effective measures as a first priority to contain and control such damage while completing all legally required reporting and other obligations.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Following in the footsteps of the GDPR, China has made tremendous legislative efforts in data and cybersecurity related laws and regulations. Some high-profile pieces of legislation and investigation cases have conveyed strong messages to companies operating in China. We have seen many leading companies make good progress with regard to improving their cybersecurity preparedness.

First and foremost, the best practices are to comply with governing laws and regulations. Therefore, it is advisable to assess a company's actual compliance work against the laws and regulations and take measures to fix any gaps.

In addition to the mandatory laws and regulations, a company may need to comply with national and industry specific cybersecurity standards, including some technical standards as guidelines for their cybersecurity work. Typical examples include the Information Security Technology standards formulated by the National Information Security Standardization Technical Committee.

The Cybersecurity Law encourages companies to take security certifications. By going through the certification process, a company can evaluate its own practices against the certification standards, and make changes accordingly to improve cybersecurity. Internationally recognised certifications including without limitation ISO/IEC 27001 are being widely adopted by Chinese organisations as well.

As the regulatory framework in China on cybersecurity is still at a nascent stage, it is advisable to closely monitor the legislative process and implementations of the laws and regulations and potential impact over a company's business operations.

In terms of implementation of cybersecurity measures, companies need to mobilise resources to cover different areas. For example, they need to upgrade their IT infrastructure to maintain a high degree of cybersecurity; employ sufficient qualified technical staff; draft and implement necessary internal policies, especially an incident response policy; adjust the governance structure by appointing a data protection officer or similar roles; and seek readily available legal, forensic,

technical and public relations advice both in the case of an incident and in their daily operation.

If any incident has escalated to a certain degree, companies tend to form a special task force with in-house legal and technical staff and, if necessary, outside counsel as well, to address such incidents. It will help diffuse the situation in a professional and efficient way before it gets out of control.

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

Cloud services are one of the fastest growing areas in China in recent years. There are many factors for a company to consider and evaluate before it makes a decision to move data to a cloud hosting environment. These factors include, but are not limited to, security, flexibility, expansion capability, performance, cost, legal compliance, etc. If a company decides to go the cloud, the general recommendation is to assess the possibility of constructing the company's own private cloud system or to deploy hybrid cloud, and only if both are unrealistic, consider the public cloud.

Photo: shutterstock.com/asharkyul

"A customer's credit card number will be stored on the private cloud with higher security protection. In contrast, official website content can be stored on the public cloud with less security protection. Such a hybrid cloud solution may also help the company to meet various compliance requirements balanced with cost concerns."

With respect to special data security and privacy concerns, a company should evaluate such concerns in a larger context to determine the most suitable cloud service. As public cloud services cover a huge volume of users and multiple business models, they are more vulnerable to hacking. Hardware sharing is common for the public cloud. This means competitors using the same cloud services may share the same server. Further, the public cloud may not always meet certain compliance requirements, such as local storage of data. In contrast, a private cloud allows a company to deploy appropriate security measures as it sees fit, which will offer a higher degree of security. It is comparatively easier to meet compliance requirements using a private cloud. But the cost for a private cloud is also higher than the public cloud. Therefore, a company must strike a balance between the competing values of relevant factors in choosing cloud services.

In China, leading public cloud service providers include Alibaba, Tencent, Huawei, China Telecom and AWS. Although private cloud service providers, such as Huawei and Lenovo, are also available, the main users of private-only cloud services are comparatively limited to financial institutes in China. For companies with data security and privacy concerns, they tend to separate data into different categories based on the security grades. For example, a customer's credit card number will be stored on the private cloud with higher security protection. In contrast, official website content can be stored on the public cloud with less security protection. Such a hybrid cloud solution may also help the company to meet various compliance requirements balanced with cost concerns.

A company shall closely monitor sector-specific regulations and standards with respect to cloud deployment. For example, the MIIT has published multiple recommendatory standards (non-binding) for the telecoms sector since mid-2021. The People's Bank of China (PBOC) has also published three recommendatory standards regarding cloud computing for financial institutions in late 2020.

Subject to its business model, a company shall closely monitor data security and privacy related laws and regulations. It shall design its core products or services from the beginning of its operation with a concept of categorised separation of data in accordance with applicable laws and regulations. This will prove more efficient and cost-effective for the company when it decides to go on the cloud later.

As most tech companies operate across national borders, cross-border transfer of data is a key concern. Companies in certain sectors (eg, financial institutions, credit business agencies, insurance companies, medical institutions, ride-hailing service providers, and smart cars) are subject to data localisation requirements. In particular, CII operators may only transfer personal data and 'important data' out of China if they have completed the security assessment organised by the supervisory authority. The party initiating such transfer shall be the responsible party to carry

out the security assessment with the other parties to provide necessary assistance. However, the detailed implementation rules for such security assessment are still pending at the time of writing (see question 1).

Another notable concern is that cloud services are not entirely open for foreign investors in China. Foreign cloud service providers may need to cooperate with local partners to step into the China market. Therefore, users of cloud service providers with a foreign background need to consider the business model of the service provider and consider whether it will have any impact on the services requested.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The Chinese government takes serious cybersecurity threats and criminal activity seriously.

The CAC is the main regulator with first-hand knowledge of market trends and cybersecurity threats through law enforcement activities, based on which it will lead the promulgation of new or amended regulations to address such concerns.

Owing to the rapid development of mobile technologies, CAC and other competent regulators such as the MIIT, the Ministry of Public Security and the State Administration of Market Regulation have focused their law enforcement efforts in regulating mobile applications in recent years. These regulators have the authority under the law to request application stores to suspend or remove download channels for illegal applications.

If any criminal offence leads are discovered during their investigation or review, such cases will be referred by the CAC to the police to initiate criminal investigations. Individual citizens or entities, especially those victims of cybersecurity threats, are also encouraged to report crimes to the authorities.

The National Computer Network Emergency Response Technical Team/Coordination Center of China (also known as CNCERT/CC) publishes annual cybersecurity reports in China. In its 2021 half year report published in July 2021, CNCERT summarised the overall cybersecurity conditions in China, specific areas of cybersecurity issues (eg, malware, website security, cloud platform security, industrial control system security) and government responses and handling of security breaches. Law enforcement actions against cybersecurity threats are increasing, with targeted campaigns on a regular basis. Civil lawsuits and public interest lawsuits against cybersecurity breaches are also increasing.

There are likely to be criminal liabilities for data violations. According to China's Criminal Law, criminal penalties for computer hacking-related offences range from three- to five-year, or even longer, imprisonment sentences. For other crimes (eg,

fraud, theft and embezzlement) conducted via cybersecurity breaches, penalties for the same crimes (conducted in a traditional offline matter as set out in the Criminal Law) will also apply. In addition, the Draft Law on Anti-Telecom and Internet Fraud was submitted to the Standing Committee of the National People's Congress for first reading in October 2021 and the second reading is scheduled in late June 2022. This new Law aims at preventing and combating relevant crimes by telecoms, finance and internet regulations.

The Supreme Court and Supreme Procuratorate jointly issued the Judicial Interpretations on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to the Information Network, which took effect on 1 November 2019. These judicial interpretations include quantified thresholds for punishable criminal offences, which provide guidelines to the police and prosecutors nationwide. The Supreme Court and provincial high courts regularly publish model cases in relation to cybersecurity crimes to raise public awareness and deter future offences. Although China does not have a case law tradition, to some degree these model cases also serve as precedents for lower-level courts to

"The Supreme Court and Supreme Procuratorate jointly issued the Judicial Interpretations on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to the Information Network, which took effect on 1 November 2019."

rule on cases. As cybersecurity crimes tend to involve a large number of victims, the police and prosecutors usually take priority in handling these crimes.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

The risk factors vary for different M&A deals. For asset or equity deals with high privacy and data security concerns (eg, purchase of software with heavy collection of user data or the equity of a hotel chain with large customer check-in data or equities of a manufacturer with a large number of employees worldwide, among many other examples) privacy and data security liabilities should be a key, if not a deal-breaking, factor.

There are several steps to follow in order to minimise potential risks. First, a proper legal and technical due diligence must be done by the buyer. This is especially important for foreign investors who are not necessarily familiar with the relevant data implications in the China market. Often this exercise should be done against not only the Chinese law, but also the relevant laws to all the jurisdictions involved (eg, the portfolio companies have a cross-border structure established for capital financing reasons, or the investors have limited partners from different jurisdictions) which may trigger, among other things, cross-border data transfer concerns (again China has strict rules around cross-border data transfer). Note the due diligence findings may prove a no go, and if that is the case, of course the earlier the finding is made, the better for both parties. Second, subject to the due diligence findings, some rectification measures shall be taken either before signing, or as closing conditions or post-closing covenants (depending on circumstances). The buyer should consider requesting a reduction in the valuation of the target, escrow arrangement, etc, to hedge against potential liabilities. Certain representations and warranties should be customised with certain carveouts to reflect the due diligence findings. Third, subject to the magnitude of potential legal liabilities due to violations of privacy and data security, the buyer may insist on special compensation (which can be as severe as, for example, reversing the deal or down to the personal liabilities of the individual sellers) or offset of remaining payments (in the case of a payment schedule in several tranches with some payable after closing). Fourth, the buyer should consider relevant insurance policies to cover liabilities for privacy and data security violations.

From the seller's perspective, it is important to shortlist credible buyer candidates. Once serious negotiations have commenced with selected buyers, the seller shall provide full disclosure to the buyers under a satisfactory confidentiality agreement. Properly documented full disclosure is the right defence for any subsequent

buyer claim after closing. Further, as a general rule in M&A deals, the seller should consider setting certain time limits to provide any compensation, including for privacy and data security violations. Needless to say, operating in a compliant way (especially navigating the dynamic Chinese data law) from day one is important for the seller.

Jingyuan Shi
jingyuan.shi@simmons-simmons.com

Yuchen Lai
yuchen.lai@simmons-simmons.com

Simmons & Simmons
Hong Kong and Shenzhen
www.simmons-simmons.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Each law firm has its own focused practices. Clients should seek cybersecurity advice from lawyers who have a long-term track record of experience in navigating cybersecurity and data protection with a legal and a sectorial eye where relevant to the client. As cybersecurity often goes beyond national borders and more importantly nowadays data legislations from the key economies globally are influencing each other so heavily (especially the GDPR's impacts globally), lawyers with international practice and experience can offer more solid advice and input from a comparative perspective. Clients should evaluate a lawyer's observations on the latest legal and regulatory development for cybersecurity from international and regional perspectives as good lawyers are always on top of the latest legal developments. Last but not least, reputation or comments on lawyers generated from previous deals may also be key attributes clients should look for.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

There are multiple layers of laws and regulations on cybersecurity and privacy in China. Some have only recently been adopted and without any detailed implementation rules, some may be in the draft stage, and the cybersecurity and privacy related legal framework is evolving at extremely fast pace, with new legislations or drafts coming out almost every month. We anticipate that this trend will continue in the next couple of years. In addition, multiple regulators may be in charge of the supervision of the same issues from different perspectives. Therefore, a client needs expert advice to help correctly analyse their case and navigate in the complex legal and regulatory framework for cybersecurity and privacy compliance in China.

How is the privacy landscape changing in your jurisdiction?

The triangulated safeguard for data regulation, ie Cybersecurity Law, the Data Security Law and the Personal Information Protection Law, are all in place. Lower-level implementation regulations and recommendatory national standards will be drafted or amended accordingly. Key regulators will finalise their internal guidelines on law enforcement where applicable. All of these changes will shape the privacy

Germany

Daniel Rücker is a partner in Noerr's Munich office. He specialises in information technology law and data protection law and heads the Noerr data privacy group. Besides complex data protection law matters such as the structuring of international data flows, he supports clients in privacy by design as well as in the context of data breaches and data protection litigation.

Sebastian Dienst is an associated partner based in Noerr's Munich office and a member of the data privacy and digital business practice groups. He specialises in data protection law and IT law. Sebastian has wide-ranging expertise in advising international companies from various industry sectors, especially in the areas of data protection governance, data protection by design, data breach management and data protection litigation.

Pascal Schumacher is a tech lawyer and associated partner with Noerr's data privacy group. Based in Berlin, Pascal focuses on regulated industries and data protection. He has particular industry expertise in the infrastructure, telecoms, banking and e-health sectors. His work includes digital platforms, privacy governance and litigation, and complex data and tech agreements.

David Bomhard is a physicist and lawyer specialising in legal advice in connection with digitisation of processes and complex IT projects (especially IT outsourcing, cloud computing, agile software development, automation of corporate processes, and use of artificial intelligence). One of his key focuses is on IT and cloud outsourcing at BaFin-regulated companies (especially insurance companies and banks).

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

On 28 May 2021, the German IT Security Act 2.0 came into force. The new law is intended as a legal basis for the federal government's cybersecurity strategy and to improve information security in Germany. This is accompanied by a massive expansion of the staff of the Federal Office for Information Security (BSI). Essentially, the German IT Security Act 2.0 pursues four goals: strengthening the role of the BSI; expanding the content of obligations for operators of critical infrastructure and other companies in the special public interest; introduction of a uniform IT security label to protect consumers; and strengthening the state's protective function.

One of the most significant changes is that the Act on the BSI (BSIG) now also provides for special obligations for 'enterprises in the special public interest'. This initially includes companies that are of considerable economic importance for Germany or that are of essential importance for such companies as suppliers because of their unique selling propositions (see section 2(14) BSIG).

IT security is not only a focus at national level but also a high priority for the European Union. In terms of IT security, the EU legislator has primarily set standards for the entire EU with the NIS Directive (EU) 2016/1148), which was already implemented in the German BSIG in June 2017. Meanwhile, a revised NIS 2 Directive is emerging. On 13 May 2022, a political agreement was reached on this. The NIS 2 Directive is now subject to formal approval by the European Parliament and the Council. In particular, it is becoming apparent that the NIS 2 Directive will expand the current scope by adding new sectors and services as essential or important entities (eg, providers of public electronic communications networks and services, digital service providers such as social networking services platforms, food businesses, healthcare providers, postal service providers and operators of ground-based infrastructure that support the provision of space-based services). Also, the NIS 2 Directive will provide for minimum standards for a regulatory framework of cybersecurity risk management measures for companies (eg, risk analysis and information system security policies, incident handling including a process for incident reporting, supply chain security and the use of cryptography and encryption).

In all likelihood, the German IT Security Act 2.0 will also soon have to be adapted to the new NIS 2 Directive in scope and measures.

IT security and cloud applications are also increasingly in the focus of the German Federal Financial Supervisory Authority (BaFin). The main purpose of the financial supervisory regulations on digital outsourcing is to prevent financial institutions and insurance companies from losing the ability to control or steer, as this could impact control by the supervisory authorities. Where activities and processes


Daniel Rücker


Sebastian Dienst


Pascal Schumacher


David Bomhard

"Controllers must notify any personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to natural persons."

are outsourced, the supervised enterprise thus continues to be responsible for compliance with all applicable statutory provisions. Regulatory standards regarding IT security in the financial sector are subject to strong dynamics, which places high demands on the monitoring of the legal situation by supervised companies.

Numerous guidelines can be found at national and European level, which provide detailed specifications of the legal requirements for cybersecurity standards.

Banks and financial institutions must, among others, comply with the requirements of the European Banking Authority (EBA) guidelines on outsourcing, which entered into force on 30 September 2019. They should complete the documentation of all existing outsourcing arrangements, in line with these EBA Guidelines already now, in certain cases by no later than 31 December 2021. At the national level, banks must comply in particular with the circular concerning new minimum requirements for risk management (MaRisk) last updated by BaFin on 10 August 2021.

With regard to insurance companies, the new European Insurance and Occupational Pensions Authority (EIOPA) Guidelines on outsourcing to cloud service providers apply from 1 January 2021 to all cloud outsourcing arrangements entered into or amended on or after this date. Insurance companies should review and amend existing cloud outsourcing arrangements related to critical or important operational functions or activities accordingly with a view to ensuring compliance with these EIOPA Guidelines by 31 December 2022. At the national level, insurance companies must comply in particular with the circular concerning supervisory requirements for IT services in the insurance sector (VAIT) last updated by BaFin on 3 March 2022.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

There are two key factors that organisations must assess when deciding whether to notify supervisory authorities and data subjects. (i) What data protection role does the organisation have for the personal data that is affected by the personal data breach: controller or processor? (ii) What risks for data subjects result from the personal data breach?

Controllers (ie, entities that decide the means and purposes of the processing of personal data) are subject to risk-based notification and communication obligations. According to article 33(1) GDPR, controllers must notify any personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to natural persons. According to the wording of the law, even personal data breaches that result in a low risk would have to be notified.

In practice, however, German data protection authorities seem to understand the term 'unless the personal data breach is unlikely to result in a risk' as 'unless the personal data breach only results in a low risk'. Against this background, some German supervisory authorities do not expect controllers to notify personal data breaches with only low risks.

Controllers must notify personal data breaches without undue delay and, where feasible, not later than 72 hours after having become aware of it. Where the notification to the supervisory authority is not made within 72 hours, it must be accompanied by reasons for the delay (article 33(1) GDPR). When a personal data breach is likely to result in a high risk to data subjects, controllers must communicate the personal data breach to the affected data subjects without undue delay (article 34(1) GDPR). Where such individual communication would involve disproportionate effort, controllers must issue a public communication or take similar measures whereby the data subjects are informed in an equally effective manner (article 34(3)(c) GDPR).

Processors (ie, entities that process personal data exclusively on behalf of one or more controllers) are not required to notify personal data breaches to supervisory authorities or communicate personal data breaches to data subjects. However, by law, processors must notify controllers without undue delay after becoming aware of a personal data breach (article 33(2) GDPR). Typically, this notification obligation is also included in data processing agreements between controllers and processors.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

One of the biggest issues that companies have to deal with when it comes to personal data breaches is to identify any security incidents in the first place. In particular, this requires raising awareness and training employees on a regular basis to ensure that employees recognise security incidents and report such incidents internally.

Another major issue for organisations in practice is gathering the relevant facts on the security incident to determine whether an incident actually qualifies as a personal data breach, which may require notification to supervisory authorities and communication to data subjects. In particular, as the GDPR does not provide specific instructions and reliable criteria for the assessment of the risks of personal data breaches, also the risk assessment is also proving to be a big challenge for many organisations in practice.

As already pointed out above, controllers must notify data breaches without undue delay and, where feasible, not later than 72 hours after having become aware of it. These quite short statutory deadlines for notifications pose major challenges for organisations in practice. To be able to be able to meet these challenging

Photo: shutterstock.com/Mistervlad

notification obligations, organisations require robust and reliable data breach management processes. Such processes should be defined in a dedicated data breach policy that clearly outlines the essential steps to manage any data breaches. The processes should be tested in 'fire drills' on a regular basis and improved based on the results of these exercises.

In order to mitigate possible adverse effects of any personal data breach, organisations must take appropriate measures as soon as possible. In particular, organisations may avoid communication obligations towards data subjects if subsequent measures ensure that any high risks to data subjects are no longer likely to materialise (see article 34(3)(b) GDPR). In order to be able to take the necessary steps right away, organisations have to be well prepared for dealing with personal data breaches. Again, this requires robust and reliable data breach management processes that should be laid down in a data breach policy.

When notifying personal data breaches to supervisory authorities and communicating personal data breaches to data subjects, organisations must disclose rather comprehensive information on the incident at hand. The notification to supervisory authorities and communication to data subjects must include a description of the

nature of the personal data breach, a description of the likely consequences of the personal data breach as well as a description of the measures taken or proposed to be taken by the controller to address the personal data breach (see articles 33(3) and 34(2) GDPR). The communication to data subjects must be in in clear and plain language (article 34(2) GDPR).

Controllers must document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance (article 33(5) GDPR). In order to meet these requirements – also in light of the statutory accountability obligation (article 5(2) GDPR) – controllers must comprehensively document any personal data breaches, even where the breaches do not require notification.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

A key issue and prerequisite for improving cybersecurity preparedness is that companies know their IT-systems, business processes and the data involved as well as relevant service providers involved. This knowledge allows them to assess the relevant risks associated with particular data, systems and processes and to take appropriate measures on the basis of a risk-based approach. Although, at least to the extent personal data are involved, the GDPR requires companies to document all that information, in practice, in our experience many companies have serious backlogs in that regard.

Based on a profound knowledge of their relevant systems, data and processes, companies strive to improve cybersecurity and the hardening of their systems from a mere technical point of view. In that context, they have to consider the various legal requirements for adequate IT security, not only GDPR requirements but also industry- and sector-specific requirements as already detailed above.

Beyond that, companies work out emergency plans. In that context, they also need to identify the individual legal requirements to be considered in the event of an emergency. From a GDPR point of view, it is essential to have a data breach policy and additional standard operating procedures with detailed guidance on who has to do what in which sequence. The relevant steps and measures to be taken need to be described in a way that is easy to understand and, even under stress and pressure, can be executed step by step. That also includes practical criteria for assessing whether a cyber incident actually involves a personal data breach, criteria for assessing the risk of a personal data breach, for whether a data breach has to be notified the data protection authorities and on whether also data subjects have to be

"It is essential to have a data breach policy and additional standard operating procedures with detailed guidance on who has to do what in which sequence. The relevant steps and measures to be taken need to be described in a way that is easy to understand and, even under stress and pressure, can be executed step by step."

informed. Notification obligations to authorities, in particular the BSI, can also result from the German IT-Security Act as well as other industry specific requirements, for example, in the fields of banking and insurance. The involvement of and cooperation with police and public prosecutors should also be considered in emergency plans as they will often be involved in context with cyberattacks. Furthermore, insurance topics have to be considered, in particular guidance on whether and to what extent relevant insurances exist, when and how insurers have to be involved and what other obligations have to be considered in order to not endanger insurance coverage. For ransomware attacks, it has to be considered whether ransom payments infringe national or international laws, in particular sanctions under EU and US law for facilitating ransomware payments. From a company law point of view, an emergency plan should require guidance on whether and when ad hoc information may need to be issued in the event of a cyberattack.

Last but not least, employees have to be trained on emergency plans, and companies are well advised to also simulate actual emergencies to further improve their cybersecurity preparedness.

Photo: shutterstock.com/SinaEttmerPhotography

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

The use of cloud services by both private and public organisations is on the rise in Germany, like everywhere else. The advantages are obvious: Cloud services allow ubiquitous data access for employees around the world, they are often more cost-efficient than building a local server infrastructure and many cloud providers are today highly reputable and ensure the highest levels of security, availability and redundancy. On the other hand, a company should also weigh the risks when considering whether to rely on external cloud systems for the hosting of personal data. In particular, cloud providers are popular targets for cyberattacks, which may create additional risks for data security and privacy. In our experience, organisations should consider two important aspects: where the cloud servers are located and how the data is protected (ie, whether the provider offers sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement state of the art technical and organisational measures).

From a data protection law perspective, cloud services are typically considered a form of controller–processor relationship. The parties are therefore required to conclude a data processing agreement (article 28 GDPR). The controller and processor may choose to negotiate an individual contract containing the compulsory elements set out in article 28 GDPR. Alternatively, the parties can use, in whole or in part, standard contractual clauses that the Commission recently adopted in June 2021 (see article 28(7) GDPR).

The use of cloud services often involves data transfers to recipients outside the EU which is subject to particular restrictions. The GDPR (articles 44 et seqq.) require the data exporter and the data importer to rely on a *numerus clausus* of transfer mechanisms, of which in the context of cloud services standard contractual clauses (SCCs) are probably the most relevant. This is true in particular since the CJEU invalidated the EU/US Privacy Shield in its *Schrems II* judgment of July 2020. But the CJEU's ruling also put international transfers based on SCCs under pressure. According to the Court, data exporters must ensure that importers are able to guarantee the inviolability of the received data, which primarily depends on local surveillance laws and government competences for access to personal data.

Partly in response to this unsatisfactory legal situation, the EU Commission has now published new SCCs for transfers to third countries (article 46(2) (c) GDPR), replacing the previous versions from 2001. For controllers and processors currently using previous sets of SCCs, there is a transition period of 18 months. Even though the new SCCs contain a provision dealing with the effects of local laws on the compliance of data transfers, due to their nature as contractual clauses they

"For certain sectors the use of cloud hosting services is subject to specific regulations. For the use of cloud services by financial services providers, for example, the Federal Financial Supervisory Authority has issued guidance addressed to all regulated financial services providers."

ultimately cannot resolve conflicts with mandatory local law of third countries. Thus, even on the basis of the new SCCs, data exporters will not be able to avoid checking in detail which surveillance laws the data importer is subject to and whether these laws affect the obligations under the SCCs. For this purpose, it is indispensable to analyse the specific data transfers in detail and to determine which laws of the third country apply in each case.

For certain sectors, the use of cloud hosting services is subject to specific regulations. For the use of cloud services by financial services providers, for example, the Federal Financial Supervisory Authority (BaFin) has issued guidance addressed to all regulated financial services providers. Under that guidance, the use of cloud services by financial services providers is not permitted to result in a situation where the responsibility for the outsourced activities and processes is delegated to the cloud provider. Where activities and processes are outsourced to a cloud provider, the financial services provider continues to be responsible for compliance with all applicable statutory regulations. To that end, the guidance suggests a number of requirements for terms that should be included in the cloud services agreement, for example, in terms of information security, authorisation management, emergency measures and control rights. This also includes that the cloud services provider must commit to cooperate with the supervisory authorities, including tolerating any on-site inspections. If the cloud provider does not agree to such terms, the financial services provider will be precluded from using the cloud for important functions.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

Following the increase in cybersecurity threats in recent years, the German government has started to implement systems and strategies addressing this growing concern. Central to formulating measures against cybersecurity threats is the BSI. Its role ranges from developing and enforcing binding IT security standards, raising awareness for the importance of internet security among the population as well as protecting federal networks and the German industry against attacks and vulnerabilities.

The BSI has published a cybersecurity strategy, which outlines Germany's position regarding cyber threats, the roles of each institution and long-term goals. The latest strategy was published in 2016 and was revised in 2021, highlighting 30 measures in the following four fields of action: (i) increasing digital awareness/competencies, such as introducing two-factor authentication and other consumer-friendly cybersecurity measures; (ii) increasing cooperation between the state and the industry, such as creating 'risk assessment' processes for companies

to assess their own risk for cyberattacks as well as creating cybersecurity certifications; (iii) creating effective and sustainable state infrastructure for cybersecurity by creating a clear course of action on how to deal with software vulnerabilities; and (iv) actively engaging with European and international cybersecurity politics to fight cyber crime.

Apart from the BSI, there are several other institutions that address cyber crime. This includes the National Cyber Defence Centre, which was established in 2011 to identify and respond to attacks on governmental and economic IT-infrastructure as well work with the German government in creating more effective preventative measures.

Another important agency to highlight is the Central Office for Information Technology in the Security Sector (ZITiS), which was founded in 2017. ZITiS is neither a police nor an intelligence agency, and has no regulatory powers but rather acts as a service provider for the security and intelligence authorities in Germany and supports them by pooling technical expertise in the areas of telecommunication surveillance, digital forensics, cryptanalysis and big data analysis.

Finally, the National Cyber Security Council plays a key role in consulting the government in terms of its strategic orientation in fighting cybercrime and comprises different stakeholders that provide balanced perspectives to the government.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

In our experience, it is still common among advisers and companies to underestimate risks resulting from privacy and data security issues in M&A deals. These issues are often at the (commercial) heart of a transaction and therefore essential for long-term success and post-closing integration.

In our view, the most relevant factors for a risk-adequate approach to privacy and data security in M&A transactions can be summarised as follows.

First, it is essential early in the M&A process to understand the business model of the target company and the details of how it has structured data processing in its commercial operations. This requires a thorough due diligence of the target's IT systems and commercial operations to determine whether personal data, in particular customer data, is lawfully collected and to identify potential limitations in using the data as intended post closing. Against the background of increased cyberattacks, due diligence should also pay particular attention to whether business secrets, critical know-how and personal data have been properly protected by the target and its group of companies. Valuations of companies more and more critically depend on IT security and intruders are becoming increasingly sophisticated.

Photo: shutterstock.com/FooTToo

Any and all issues should be addressed through appropriate and custom tailored language in the representations, warranties and post closing undertakings in the deal documentation.

The second area concerns the structuring of the (bidding and) transaction process. Setting up a straightforward risk-sensitive and compliant privacy structure for the transaction process early on is in our experience a top priority. Privacy related workstreams already start with the selection of the data room provider, the structuring of access levels and content, and setting up clean teams agreements for particularly sensitive documents. In later phases of the transaction, for example, issues ranging from employee and customer communications to migration preparation and migration play an important role.

We recommend setting up a data protection "step plan" at an early stage to define and document the legal basis for each data transfer within the transaction and coordinate such step plan with all parties involved. Letting this slide regularly leads to unpleasant surprises in the critical phase between signing and closing, eg when a company invokes data protection compliance to inform customers about the

deal while another party insists on confidentiality so as not to jeopardise the deal in the home stretch.

Particularities arise in international M&A deals, which can involve the transfer of large amounts of personal data outside the EEA. Companies should make sure that they process such data in full compliance with the GDPR.

Daniel Rücker
daniel.ruecker@noerr.com

Sebastian Dienst
sebastian.dienst@noerr.com

Pascal Schumacher
pascal.schumacher@noerr.com

David Bomhard
david.bomhard@noerr.com

Noerr
Berlin and Munich
www.noerr.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Clients should assure that their counsel is familiar with all the relevant different kinds of issues that may be involved in cyberattacks. The counsel involved should be used to cooperating with the relevant authorities in order to solve issues as smoothly as possible to client. Clients should involve a firm that holds available a cyber risks team with specialists in all different areas of law involved that is able to react quickly and that cooperates seamlessly and efficiently.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

Different interpretations of the legal requirements and different enforcement practices of 18 individual data protection supervisory authorities at a German federal and state level makes advising on data protection law in Germany even more interesting.

The relevance of contract drafting is increasing. Outsourcing and cloud contracts must strike the right balance between customer-specific cybersecurity requirements and established service provider standards.

How is the privacy landscape changing in your jurisdiction?

The privacy landscape is still characterised by a large number of unresolved legal issues and a constantly evolving practice. Companies should closely monitor the legal developments and update processes and documentation. Claims for damages following breaches of data privacy were initially rarely enforced; however claimant-friendly case law has been established on non-material damages following data privacy breaches. Exclusion of liability for minor damage is often no longer considered, and some courts find a victim's feelings to be damage.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

We have seen a growing number of ransomware attacks. Some of these attacks are prepared very well in advance. One of the most important precautions for companies to mitigate such scenarios are reliable, safe and frequent data backups.

Greece

Elina N Georgili is head of the data protection and privacy practice at KG Law Firm. She has extensive experience in data protection and specialises in privacy, confidentiality and security issues. Elina has headed important data protection compliance projects in various industry sectors, represented clients before the Greek and foreign data protection authorities, provided legal advice to multinational corporations and groups and drafted Codes of Conduct and important legal opinions. She participates in various legal forums and privacy and banking professional associations and has authored various articles and other publications. Elina acted as member of the Greek Committee for Drafting the Code of Conduct for Lawyers.

Natalia Soulia is a senior associate in the data protection and privacy practice group at KG Law Firm. Her practice, spanning advisory, public policy, transactional and contentious work, focuses on all aspects of data protection law, with an emphasis on the technology and financial services sectors. Natalia provides strategic legal advice on privacy and e-commerce issues, while she has also participated in multiple due diligence investigations, GDPR compliance and cybersecurity assessment projects and internal audits.

Evangelia Brinia joined the data protection and privacy practice at KG Law Firm. Her areas of expertise on data and privacy originate from a business approach and a theoretical compliance perspective. Her thorough practice field knowledge derives from both current legislative framework study and legal business orientation. She has gained experience through coordination of GDPR compliance projects, drafting of policies and handling matters before the Hellenic Data Protection Authority.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

On 4 June 2021, the Greek National Cybersecurity Authority (NCA) issued the Cybersecurity Manual, which contains the best practices proposed in order to boost the level of organisations' cybersecurity preparedness.

In line with the Manual, the Digital Transformation Bible 2020–2025 was issued by the Greek Ministry of Digital Governance in June 2021, thus contributing to the formulation of a national strategy on digital transformation. The most important pillars of the new strategy are based on: (i) public administration reform in order to promote access to easy-to-use digital services; (ii) bolstering of private initiative for the use of new digital services; (iii) promoting implementation of new digital tools; and (iv) investing in the digital training of human resources.

2022 is considered to be a milestone year according to the Greek National Cybersecurity Strategy of 2020–2025. During this year, the strategic axes of an integrated Greek cybersecurity policy are expected to be established. These include:

- updating the National Cybersecurity Strategy and developing an action plan;
- developing a cybersecurity best practices handbook;
- preparing a risk assessment study on a national level;
- preparing a cyber crisis management and continuity plan;
- carrying out awareness-raising activities (seminars, workshops, etc) on cybersecurity;
- establishing a platform to protect websites against cyberattacks;
- establishing a platform and a toolkit for vulnerability assessment and penetration testing;
- developing a of cybersecurity R&D agenda;
- developing cybersecurity investment toolkit; and
- establishing a system for monitoring the availability of the websites of governmental organisations and critical infrastructure.

Further, this year marks the operation of the first centralised electronic applications and centralised information systems used for the electronic identification and authentication of citizens (Greek Law 4624/2019) as well as of the Central Internet Portal of the Greek state, which enables citizens' access to public sector services (Greek Law 3979/2011).


Elina N Georgili


Natalia Soulia


Evangelia Brinia

"Each company should adopt a dedicated data breach management policy and procedure."

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

A data breach constitutes a security incident affecting a company's organisational structure and protection systems, which may lead to the unlawful destruction or loss of data processed by the company, thus impacting on its proper operation and reputation.

According to article 33 of the GDPR, a data breach is required to be notified to the competent supervisory authority when it poses a high risk to the rights and freedoms of the data subjects concerned. Notification to the competent supervisory authority should be made without undue delay and in all cases within 72 hours of the data controller becoming aware of that breach. In addition, in accordance with article 34 of the GDPR, in the event that the data breach is likely to present a high risk to the rights and freedoms of the data subjects concerned, the company must also communicate the breach to those data subjects affected thereby immediately.

To mitigate these risks, each company should adopt a dedicated data breach management policy and procedure, on the basis of which it will be able to assess the risks arising from a security incident in order to decide whether to notify the data breach to the competent supervisory authority and whether to communicate it to the data subjects affected. Furthermore, in light of the principle of accountability as enshrined in article 5(2) of the GDPR, the company should comprehensively document any personal data breaches that occur, whether or not such data breaches require notification.

The key factors that a company should assess in order to decide whether to notify a security incident to the competent supervisory authority and to the affected data subjects are primarily the nature of the personal data affected and the severity of the risk resulting from that breach. The company should also consider the technical and organisational measures implemented as soon as it becomes aware of the data breach, in order to prevent or reduce the risk arising to the freedoms and rights of the persons affected.

It is required that the data protection officer (or the other competent persons) make a proper assessment of the factors leading to the notification of a data breach to the supervisory authority or to the data subjects affected, or both, as the data controller has the dual obligation of ensuring compliance with the data protection legal framework and mitigating any reputational damages as a result of the publicity that the data breach may receive.

Photo:shutterstock.com/Tampa

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

Proper and secure data processing is vital for a company's operation, reputation and continuity. Despite the existence of a robust legal framework on the protection of personal data established by the GDPR, the risk of security incidents affecting company data is constantly increasing.

Companies typically have to protect two major types of data: business-critical data, comprising the data assets needed the company's operation, and private information, which includes employees' personal data (eg, payroll data and health data), customer and third party personal data, etc.

The biggest issue that a company has to deal with when it suffers a data security incident is to protect the corporate and personal data in its possession that are affected by this incident. To this end, the company should adopt dedicated, robust policies, such as a data breach policy and an incident response plan, which are intended to enable timely identification of security incidents and appropriate mitigation of the consequences thereof.

Against this background, the company should immediately manage the data security incident by taking at least the following steps. First, suspected or confirmed data security incidents should be reported internally (eg, to the company's DPO) in a timely manner by the employees who became aware of them. Second, a thorough investigation must be carried out by the competent persons to ascertain whether the incident qualifies as a personal data breach, which may require notification to the supervisory authority or relevant communication to data subjects, or both. For this reason, the company should assess the immediate consequences of the data breach, and perform an evaluation of the following factors:

- the causes of the incident;
- personal data affected;
- the impact to the data subjects affected; and
- a whether other company systems are threatened with immediate or future risk.

Following this assessment, there should be an immediate adoption of all necessary technical and organisational measures to mitigate consequences of the breach. In the event that the security data breach is expected to pose a risk to the rights and freedoms of data subjects, then the company should notify the competent supervisory authority without undue delay and in all cases within 72 hours of becoming aware of it. The notification to the supervisory authority should contain detailed information on the nature of the data breach, a description of the likely consequences to the data subject or other subjects affected and a description of the measures taken or proposed to be taken by the company to mitigate the risk. Where the company concludes that the security data breach is likely to pose a significant risk to the rights and freedoms of data subjects affected, it is required to communicate the breach to data subjects involved as well. Where the company has taken robust measures to ensure that the high risk to the subjects is no longer likely to materialise, communication towards the latter is not necessary.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Among the key requirements for improving cybersecurity preparedness is an inventory of hardware and software hosted on the company's physical infrastructure, as well as the secure configuration of servers, network devices and applications. In addition, restricting access to the company's information systems only to authorised users could lead to satisfactory preparedness results against any form of threat that may arise. Further, of great importance is the establishment of user authentication systems. These systems are the first targets for any cyberattacker, given that weak

> “Among the key requirements for improving cybersecurity preparedness is an inventory of hardware and software hosted on the company’s physical infrastructure, as well as the secure configuration of servers, network devices and applications.”

passwords, non-secure storage of passwords by the user and phishing could result in the theft of the user’s identity and the acquisition of unauthorised access to a company’s valuable resources. In addition, practices such as the creation of strong passwords, the implementation of two-factor authentication and screen locking after a period of user inactivity are regularly followed.

With regard to the most recent developments in the area, the majority of private companies and public organisations have now implemented a remote working model, which has fostered the appearance of cyberattacks. Developing a remote work policy, updating the VPNs and network equipment of the institution with the latest software patches and security configurations and the regular backup of files on an external storage medium (USB or external hard drive) could contribute to cybersecurity preparedness.

In addition, cybersecurity training programmes, focused in particular on how users can interact with their devices and the network in a secure manner, the awareness and detection of social engineering attacks, the recognition of the signs of system breaches and insider threats, are among the best practices applied.

Lastly, to improve cybersecurity preparedness, companies deploy information security and privacy management systems combined with technical security hardening measures.

Management systems usually refer to ISO 27001 and provide: (i) comprehensive protection of all identified information assets including trade secrets, confidential information, operational data and equipment as far as integrity, confidentiality and availability is concerned; (ii) a risk-based approach to reduce security management costs; (iii) policies and procedures to facilitate implementation; (iv) a continuous improvement approach; and (v) continuous training and awareness.

Further, they usually refer to: (i) installation of firewalls; (ii) installation of end point security for malware detection and removal; (iii) email protection by using software as a service platforms to filter incoming emails and quarantine suspected ones, (iv) AI-based user behaviour analysis systems; and (v) data backup and restore procedures and equipment. Technical measures management systems are listed as commonly used.

Photo:shutterstock.com/repetylo

5 | Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

The rapid adoption of technologies in the past couple of years, and their continuous development, has made business environments particularly prone to serious cyber-threats. Now more than ever, it is imperative for businesses to become more agile through the implementation of security policies and protocols, to achieve regulatory compliance and more importantly to improve their cybersecurity preparedness, in order to safeguard their data flows.

However, the question they need to pose is how could legal expertise facilitate their demands for security and provide them with the highest level of protection. In essence, the transfer of data outside of the organisation opens up the latter's environment for attack. Our experience has shown that aside from the vast benefits of this approach, which include its cost-effectiveness, its functional facilitation of resource management and its provision of critical threat intelligence, the inevitable fragility of data transfers requires the combined effort of security policies and legal support. To resolve this vulnerability, businesses have turned to the cloud hosting environment. From the onset, the use of cloud networks worldwide has contributed to the decrease in security breaches of least 60 per cent in the public and private sectors compared to traditional data centres. Per contra, in Greece this approach is still less popular according to a recent survey of Eurostat.

Bearung all the above in mind, from a legal standpoint it is imperative for companies to ensure their regulatory conformity with the applicable regulatory regime.

In particular, article 28 of the GDPR sets out rules on the conditions for outsourcing data processing to data processors. In this respect, companies under their authority as data controllers that use cloud computing to transfer or store personal data are required to conclude a data processing agreement (DPA) with the cloud provider, acting as a data processor, governing their internal relationship.

With regard to personal data that are being transferred to a cloud provider established outside the European Economic Area (EEA), GDPR restrictions on cross-border data transfers become applicable. Companies that transfer personal data outside the EU could rely on the new set of standard contractual clauses (ie, the company as a data controller and the cloud service provider usually as a data processor).

Beyond the aforementioned, companies should also be aware of the following considerations. To begin with, companies should be aware of the regulatory limitations on data storage outside their territory (if any).

In addition, companies should ensure that all their security policies are updated with the contribution of expert support so as to manage risks effectively. Secure

"Companies should ensure that all their security policies are updated with the contribution of expert support so as to manage risks effectively. Secure remote access is another concern for which companies need to raise their awareness."

remote access is another concern for which companies need to raise their awareness, in which case the implementation of cloud security features on the employees' devices working remotely could definitely ensure the security on a large scale, of not only their personal data, but also sensitive information of the companies' clients.

Based on our expertise, the optimal strategy that any company could implement concerning the protection of data flows outside the organisation is the adoption of a minimum encryption level by default, according to which personal data will be temporarily stored on a queuing server, considering that the cloud-based solution is the data destination.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

In light of the increase of cybersecurity threats and criminal activity over past years, the Greek government has recognised the urgency of strengthening its information security policies alongside its communication systems and networks with the purpose of protecting citizens' privacy and personal data. According to a survey by Check Point Software Technologies, cyberattacks in Greece have increased by 52 per cent since May 2020, mostly in the healthcare sector, while the Global Information Security Survey by EY stresses that during the pandemic there have been serious cyberattacks targeting not only Greece's critical infrastructure, but also intercepting important information.

First and foremost, the NCA is entrusted with, inter alia, the implementation of the appropriate organisational, technical and operational measures, (for instance, the development of security policies and procedures for the prevention of future security incidents, management of the institutional framework, crisis management and activation of the National Emergency Plan) and the coordination of other institutions that combat cybercrime. Greece has officially published its own National Cybersecurity Strategy 2020–2025 , introducing its strategic goals, highlighting the importance of collective effort and partnership between all institutions, sharing its vision to build a modern digital environment, a culture of safe use pertaining to advanced technologies in the digital era (5G networks, AI, IoT) and aiming to increase trust towards digital governance. In the context of evaluating its strategic plan, it underlined that its strategic interest was extended in six dimensions: (i) emergency planning; (ii) incident reporting; (iii) security and privacy protection; (iv) research and development; (v) partnerships between the public and the private sectors; and (vi) investments in security measures.

Following the European Cybersecurity Guidelines, the NCA developed five strategic goals for implementation. These include: (i) the existence of a functioning

system of governance, aiming to optimise the organisational framework and effective risk and emergency management; (ii) safeguarding the infrastructure, security and the newly implemented technologies, not only by deeply understanding their evolution and influence, but also through enhancing their security requirements; (iii) the improvement of the how incidents are being managed with reference to cybercrime and privacy protection, such as strengthening the deterrence mechanisms and boosting business cooperation; (iv) the creation of a modern environment emphasising promotion of research and development, where the public and private sectors will be closely cooperating; and (v) capacity building and improvement of skills through appropriate organisation exercises, while utilising modern training tools and education methods and, of course, constant updates for institutions and citizens on cybercrime threats and issues.

Except for the NCA, there are other essential stakeholders contributing to cybercrime mitigation. In principle, the National Community Emergency Response Team (in Greek, EYP) is the institution that deals with the evaluation of classified information and the assessment and certification of cryptosystems supporting military forces in cryptosecurity matters, including but not limited to prevention and warning of cyberattacks. On top of that, the EYP oversees the Computer Security Incident Response Team (the National CSIRT), having as its mission to reduce the risk of national challenges in the field of cybersecurity and communications in the event of cyberattacks on public bodies.

Furthermore, with the Presidential Decree No. 178/2014 the Cybercrime Division was established as an independent central service that reports directly to the chief of the Hellenic Police. Its mission focuses on the prevention, investigation and suppression of crime and antisocial behaviour committed through the internet or other means of electronic communication. The Division consists of five departments, complementing in this way the whole range of user protection and security of cyberspace: (i) the Administrative Support and Information Management Unit; (ii) the Innovative Actions and Strategy Unit; (iii) the Electronic and Telephone Communication Security and Protection of Software and Intellectual Property Rights Unit; (iv) the Minors Internet Protection and Digital Investigation Unit; and (v) the Special Cases and Internet Economic Crimes Prosecution Unit.

The efforts of all the above-mentioned institutions are supplemented by the Hellenic Data Protection Authority (HDPA) and the Hellenic Authority for Communication Security and Privacy, authorised with, respectively, the supervision of compliance with the General Data Protection Regulation, Greek Law 4624/2019 and Greek Law 3471/2006, governing personal data protection and privacy in the electronic communications sector.

Photo:shutterstock.com/Aerial-motion

Of equal importance is the Hellenic Telecommunication and Post Commission's (EEET) work in battling cybersecurity threats and criminal activity by regulating and supervising the electronic and wireless communications' market.

Lastly, the establishment of Government SOC (Security Operations Center) also plays a pivotal role given that includes engineers who monitor, respond and conduct threat hunting to detect and respond to arisen threats or targets and the appropriate technology, for instance, security information and event management (SIEM) platforms for correlating and analysing the complicated data points across the IT environment also contribute to the combat against serious cybersecurity threats and criminal activity.

7 | When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

Companies' compliance with the data protection regulatory framework has a significant impact on M&A deals. In particular, the due diligence process of a target company is subject to strict requirements and standards from the data protection

perspective. This is due to the buyer company facing significant risks as a result of violations of data protection legislation by the target company, which may lead to the buyer being exposed to administrative fines, civil claims and reputational damage.

In light of this, a thorough and detailed due diligence procedure should be carried out by the buyer to assess the level of compliance of the target company with the data protection framework, as well as to indicate potential red flag issues before closing, which might affect the drafting of the transaction documents. This includes a proper assessment of all documentation provided by the target company, such as relevant data protection documents (eg, register of processing activities, privacy policies, privacy notices and consent forms), data processing agreements concluded with third parties, any DPIAs concluded, information on data transfers outside the EU/EEA and information regarding any data breaches, fines and any complaints to the competent supervisory authority. Further, it is imperative that due diligence is thoroughly performed to assess whether the target company uses secure IT systems and has adopted effective measures to protect personal data processed.

Following the assessment of the data protection compliance risks, any identified vulnerabilities should ideally be rectified by the completion of the M&A deal (formulated as a closing condition). If the aforementioned risks cannot be eliminated in time, the M&A deal should contain appropriate representations and warranties with respect to the data protection legislation (as post-closing covenants) so that the buyer could claim specific compensation if data protection liabilities arise.

Elina N Georgili
e.georgili@kglawfirm.gr

Natalia Soulia
n.soulia@kglawfirm.gr

Evangelina Brinia
e.brinia@kglawfirm.gr

Kyriakides Georgopoulos Law Firm
Athens, Thessaloniki
www.kglawfirm.gr

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

To ensure the appropriate level of security, companies should address their requests to lawyers who have extensive experience in advising on data protection and cybersecurity issues, having in-depth knowledge of both the current legislative framework and the latest developments on cybersecurity and privacy, as well as a practical understanding of IT issues.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

The ever-increasing number of cyberattack incidents in businesses, especially after the increase of teleworking and the enhanced use of technology, has created a need for many businesses to take appropriate security measures and adopt policies and procedures to protect their business-critical data, as well as the personal data of their employees, partners and customers involved. In addition, there is still a number of companies in Greece that have not yet achieved compliance with the data protection rules, or that need to clarify various issues that constantly arise.

How is the privacy landscape changing in your jurisdiction?

Law 4624/2019, enacted in August 2019, expresses the intention of the legislator to regulate certain fields that the GDPR reserves to each member state, such as data processing in the employment field. This Law also incorporates Directive 680/2016/EU (concerning processing of personal data for criminal investigations and penalties). The Hellenic Data Protection Authority demonstrates great sensitivity on data privacy issues, including cookies and the employees' data during teleworking.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

The most common cyberattack identified for companies is ransomware, realised by means of blackmail. The orchestrators threaten to leak client's sensitive data, business plans and patents, fake news or corporate espionage, thus destroying the companies' goodwill. Around 80 per cent of attacks initially target the average user.

Hong Kong

Michelle Ta has a breadth of experience across technology transactions, IT outsourcing, software and IP licensing, and privacy and data protection, and she has also made achievements in the field of financial technology. She has provided a series of data-related consulting services for virtual banks and fintech clients, and is currently seconded part-time to a virtual bank in Hong Kong to provide long-term legal support. Michelle is also an experienced cybersecurity legal advisor, and has acted in-house for a global IT services giant as the company's cybersecurity subject matter expert.

Clients have described Michelle as 'one of the few lawyers I would call having the full package', 'a lawyer to watch out for in the TMT sector' and having 'excellent technical skills and great commercial judgment across banking, technology and corporate practice'. Michelle was recognised for her commercial acumen as a finalist for the prestigious Australian Financial Review BOSS Young Executive of the Year award in 2017.

Michelle is dual-qualified in Hong Kong SAR and Victoria, Australia. She graduated from the University of Melbourne with first class honours in Law and holds a second bachelor degree in science, with double majors in biochemistry and biotechnology.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

Hong Kong does not have a dedicated cybersecurity statute or mandated cybersecurity standards. However, there are a variety of sector-specific requirements for regulated businesses and cybersecurity continues to be an area of intense focus for financial regulators such as the Hong Kong Securities and Futures Commission (SFC) and Hong Kong Monetary Authority (HKMA).

For example, at the start of 2021, the HKMA implemented an upgraded Cybersecurity Fortification Initiative (CFI 2.0). The original CFI regime was launched in 2016, and CFI 2.0 is a result of the HKMA's recognition that cybersecurity is a rapidly evolving landscape. The CFI contains enhanced expectations of attack simulation testing, cyberattack readiness and cyber resilience controls. This is a continuation of the HKMA's long-held focus on protecting customer data, which continues to be a major area of focus as banks increasingly become more digital.

The SFC has also been working to bolster its cybersecurity expectations. In 2020, it issued a thematic cybersecurity review of internet brokerages, which indicate the SFC's continuing concerns that mobile applications and other digital interfaces are more vulnerable to hacking risks and security breaches than traditional forms of interfacing with clients. The SFC has called out encryption, user access management and tracking of data access as particular areas of focus (and this is also consistent with the focus of parts of the SFC's introduction of more stringent cloud storage requirements over the past couple of years). More recently, the SFC has also used further guidance on managing the cybersecurity risks of remote working.

In terms of legal changes, the last major change occurred in 2019. Hong Kong has traditionally leveraged section 161 of the Crimes Ordinance to tackle cybercrime. Section 161 of the Crimes Ordinance deals with access to a computer with a criminal or dishonest intent, for example, with intent to commit an offence, with a dishonest intent to deceive, with a view to dishonest gain, or with a dishonest intent to cause loss to another.

Section 161 – typically understood as a hacking offence – has been used in Hong Kong over the years as a 'catch-all' offence for all manner of crimes committed using computer devices, including things like 'upskirting' (taking sexually intrusive photos so as to see up a person's skirt or dress without permission). This changed in 2019 when a Court of Final Appeal judgment (*Secretary for Justice v. Cheng Ka Yee*) confirmed that section 161 does not apply to a person's use of his or her own computer. This judgment has redefined section 161 as a provision aimed at tackling cybercrime.


Michelle Ta

While section 161 of the Crimes Ordinance currently still remains the only 'per se' cybercrime statutory provision in Hong Kong, in October 2021, the Hong Kong government announced plans to implement a new cybersecurity law to help ensure the security of Hong Kong's network information systems at a macro level, which is expected to cover important or critical infrastructure, such as government agencies, financial institutions, telecommunications facilities and public transportation facilities. The Security Bureau, being the relevant governmental department taking the lead on this, is expected to submit documents to the Hong Kong legislative council as well as launch public consultations by the end of this year, and the government has expressed that references will be drawn from cybersecurity standards adopted worldwide in formulating relevant standards in Hong Kong.

Additionally, an amendment to the Personal Data (Privacy) Ordinance (PDPO) in Hong Kong took effect on 8 October 2021 to prevent a type of cyber offence known as 'doxxing', which is the publishing of personal identifying data without consent with malicious intent. The amendments made to the PDPO seek to close a policy loophole by giving the Privacy Commissioner for Personal Data (PCPD) greater enforcement powers including powers to institute prosecutions and order the

removal of doxxing content. It has particular implications for insider threats and 'stray employee' cybersecurity risks, and for companies that allow user-generated content like social media platforms. The new anti-doxxing provisions also come with extraterritorial effect, where section 66M(2) of the PDPO now gives the PCPD power to direct a service provider, whether it is in Hong Kong or not, to take certain actions (including taking down content) in cases of doxxing. Companies (and in particular those in the TMT sector) should continue to look at and bolster external policies on platform use and internal policies on the handling of personal data and content moderation, such as developing and investing in measures to curb doxxing or provide training on how to respond to cessation notices.

Finally, the PCPD recently issued a new Guidance Note on the Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data, in which two new sets of recommended model contractual clauses (RMCs) are introduced, namely data-user-to-data user RMCs and data-user-to-data-processor RMCs. The data-user-to-data-user RMCs set out model clauses for data transfers between two data users (or data controllers) and are aimed at ensuring that a transferor takes all reasonable precautions to ensure that personal data transferred to a transferee acting in the capacity as a data user is not processed in a manner that would violate the PDPO. The data-user-to-data-processor RMCs sets out model clauses reflecting the PDPO requirement that a data user remains accountable for the acts of its data processors and imposes contractual obligations to oblige data processor transferees to comply with the requirements of the PDPO. The RMCs are recommended by the PCPD to be incorporated in agreements where personal data may be transferred outside of Hong Kong by a local entity to an overseas entity, or between two entities outside of Hong Kong where such transfer is controlled by a data user that is subject to the PDPO.

In reality, the RMCs are difficult to implement and are likely to be resisted by data processors, because they comprise certain obligations that lie beyond the control of data processors, such as requiring the transferee to ensure personal data transferred is adequate but not excessive. The actual law itself has not changed (and in particular, the relevant section of the PDPO (section 33) restricting cross-border transfer of data is still yet to come into effect with no timetable announced for its implementation). Adoption of the RMCs is therefore not mandatory. Organisations are also free to adapt and modify the RMCs or use alternative wording as long as they are consistent with PDPO requirements. As such, the RMCs are likely to be negotiated heavily by both data users and data processors, and we do not expect the same level of widespread use as that seen, for example, with the Standard Contractual Clauses under the GDPR.

"The Hong Kong government has been discussing a range of changes to the Hong Kong privacy law, including introducing a mandatory data breach notification regime."

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

There is no general mandatory data breach reporting regime in Hong Kong. While reporting of data breaches is encouraged by the Hong Kong Privacy Commissioner, as a matter of practice, we see clients take a range of approaches to voluntary reporting (whether that is reporting to the regulator or affected consumers). Usually the things that clients weigh up include whether the data breach might have to be reported on a mandatory basis in another jurisdiction (in which case, clients tend to lean to voluntary reporting in other affected jurisdictions); the size of the data breach; and the risk of harm to affected individuals. Factors such as negative public perception and financial consequences are also important considerations.

That said, since the start of 2020, the Hong Kong government has been discussing a range of changes to the Hong Kong privacy law, including introducing a mandatory data breach notification regime. While we are yet to see legislative progress regarding a mandatory data breach notification regime, we expect this to

stay high on the agenda in Hong Kong and that it will become law in the not-too-distant future.

Of course, for regulated businesses – and in particular, those businesses that are subject to the supervision of financial regulators – there continue to be sector-specific regulatory expectations to report data incidents within certain time frames.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

The biggest issues that companies need to consider from a privacy perspective arise even before companies suffer a data security incident.

First of all, data security (and privacy protection in particular) should be board-level issues. Too often, they are considered the sole domain of certain stakeholders (the CISO, a data protection officer or another 'tech' or 'legal' person) – so the first issue that companies need to address from a privacy perspective is an understanding that this is an enterprise-wide responsibility.

Photo: shutterstock/ESBProfessional

Dealing well with a data security incident starts from prevention in the first place, followed by good preparation for the worst-case scenario. The companies that do this best have a multidisciplinary team (stakeholders from senior management through to lawyers, public and government relations experts, cyber forensics professionals) that have been trained and drilled for cyber incident simulations so that they can mobilise quickly to respond to a data security incident when it (inevitably) occurs. Those companies know what steps they need to take and the order in which they need to take those steps – from initial containment of a data breach, through to ensuring key evidence is collected in a way that maintains chain-of-custody (particularly important so that digital evidence is not accidentally erased or changed in an effort to fix a breach), through to taking measures to fix vulnerabilities and post-mortem reviews. All of that will be important if a company is required to report an incident to a specific regulator (for example, the HKMA) or if the company decides it wants to voluntarily report the incident to the Privacy Commissioner or affected customers.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

There are a range of approaches in Hong Kong to cybersecurity preparedness. Banks are among those that have the highest level of regulatory expectations when it comes to cybersecurity preparedness and cyber resilience. In terms of best practice, regulated banks in Hong Kong must meet a minimum baseline of cybersecurity readiness, which is set out in the HKMA's Cybersecurity Fortification Initiative. This comprises three pillars – the Cyber Resilience Assessment Framework, which helps banks assess their cyber risk posture and benchmark their level of defence and resilience; the Professional Development Programme, which is a certification scheme for cybersecurity practitioners in the industry to boost technical capability in areas such as attack simulation testing; and the Cyber Intelligence Sharing Platform, which is aimed at sharing cyberthreat intelligence to help the industry stay informed of, and prepare for, emerging hacking tactics and patterns.

This is consistent with common cybersecurity wisdom that cybersecurity is a patchwork of defences in an organisation's people, processes and technology.

Other sectors take a range of approaches to cybersecurity preparedness, and there remains a broad spectrum of cybersecurity maturity levels in Hong Kong.

"Organisations that are supervised by the SFC in Hong Kong should be particularly aware of additional requirements imposed by the SFC on the use of external electronic data storage services (like cloud hosting services) to store their data and records."

5 | Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

Yes – in particular organisations that are supervised by the SFC in Hong Kong should be particularly aware of additional requirements imposed by the SFC on the use of external electronic data storage services (like cloud hosting services) to store their data and records. The SFC issued a Circular in late 2019, and in late 2020 a set of accompanying FAQs, setting out certain requirements for licensed corporations wishing to move their data storage to a cloud hosted environment. Some of the requirements and expectations set out in this regime impose sector-specific requirements which are unusual both in the context of cloud service agreements in a broader sector-agnostic context as well as in comparison to expectations in the same sector in other jurisdictions, including, for example, a requirement to maintain a full and immutable audit trail to memorialise access logs by every unique user of a data record.

Outside of these requirements of the SFC, there are of course all the usual requirements that businesses should consider when thinking about moving data

to an environment hosted by a third party – including due diligence to ensure the relevant cloud product is fit for the intended purpose, that the vendor is certified against prevailing industry cybersecurity standards, that the vendor can meet required data availability and uptime commitments and that there is a certain level of redundancy and disaster recovery to protect data loss. In addition, cross-border data transfer restrictions are becoming more complex for projects for moving to a cloud hosted environment touching on multiple jurisdictions. Finally, increasingly, concerns about increased exposure to excessive government or regulatory access to cloud hosted data (and in some cases, conflict of law issues) are becoming a top consideration when looking to move data to the cloud.

6 | How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

A specialist unit within the Hong Kong Police – the Cyber Security and Technology Crime Bureau – is responsible for investigating and handling technology crime, computer examinations and preventing technology crime.

In addition, as discussed in further detail above in question 1, an amendment was passed last year to reform the Personal Data (Privacy) Ordinance to combat malicious doxxing acts and protect the public's personal privacy. A raft of new enforcement powers were also conferred on the PCPD to investigate and prosecute doxxing crimes, as well as granting the PCPD with the power to issue cessation notices with extraterritorial effect.

In relation to the proposed development of a local cybersecurity law, we expect to see documents submitted to the legislative council and public consultations launched in the second half of 2022, with the aim to enhance the cybersecurity of critical infrastructure in the city through legislation that will seek to require all private and public enterprises to comply with cybersecurity regulations.

7 | When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

All companies should be doing appropriate level of privacy and data security due diligence when looking at a potential acquisition or merger target. This involves diligence from a legal perspective (eg, whether there have been any recent mandatory or voluntary data breaches notified to regulators, whether there have been any near misses and whether there have been any data handling complaints or litigation that may indicate a systemic issue), as well as from a technical perspective (eg, bringing in cybersecurity professionals to assess a potential target's cybersecurity posture).

This is particularly important for companies that engage in businesses that are data-intensive, businesses that interface directly with consumers or businesses that are subject to particularly strict privacy laws in other jurisdictions. A history of multiple or serious non-compliances with the applicable data law, spotted during the due diligence process, may affect the value, terms or indeed continuation of the deal. These risks should also factor into decisions about M&A deal shapes and ways in which sellers may be required to remain financially responsible or accept more onerous terms for latent privacy and data security issues.

Michelle Ta
michelle.ta@simmons-simmons.com

Simmons & Simmons
Hong Kong
www.simmons-simmons.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Clients should also look for curious lawyers with an in-depth understanding of technology, computers and cybersecurity as a discipline (ie, knowledge beyond the strictly legal) with a good team of litigator colleagues working alongside them to cover tricky dealings with customers or regulators. It is important to look for a team with a good working knowledge of data law across multiple jurisdictions.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

The fact that Hong Kong data law has been around for so long (since 1995!) and remains relatively unchanged today is a very interesting contrast to the pace of change in data regulation in other parts of the world – this is particularly the case because so many multinational companies have their Asia headquarters in Hong Kong, so the interplay in practice between different laws can become very complex and interesting as data itself often lives in more than one location in today's cloud-reliant business environment.

How is the privacy landscape changing in your jurisdiction?

Hong Kong's data and privacy laws definitely win the prize for longevity! They are due for a change (although I'm constantly amazed at the resilience of the PDPO and how well a law drafted in 1995 still holds up and adapts so well to so many novel practical situations in 2021). And as of 2020, we are finally seeing the beginnings of an earnest review of important areas for reform.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

In Hong Kong, phishing still remains one of the top tactics for bad actors to infiltrate systems. Threat actors are becoming more sophisticated and more patient and will wait longer to execute large-scale attacks, such as targeted emails to senior executives to trick them into transferring large sums of company.

India

Abhishek Malhotra, founding and managing partner of TMT Law Practice, has two decades of experience in the primary areas of expertise, including intellectual property, commercial dispute resolution, technology, media and telecommunications. He has advised clients in minimising legal risks and devising strategies for safeguarding against civil and criminal liability. Mr Malhotra's expertise in the media sector has resulted in a close alliance with production houses, broadcasters, and artists across the industry, and he is recognised as the 'go to' professional for issues across broadcasting, music and sports.

Mr Malhotra is a member of the Bar Council of Delhi and the State Bar of California, and holds memberships of national and international professional associations. He has contributed to books and papers on intellectual property, sports and gaming, data protection, cybersecurity and artificial intelligence.

Atmaja is a senior associate with the dispute resolution team at TMT Law Practice. Her areas of expertise include technology and media law, competition law, copyright law and constitutional law. She has represented the firm's clientele from the telecommunications, media, television, online gaming and radio broadcasting industries before courts, including the Supreme Court of India and High Courts, in and tribunals and complex arbitrations involving start-ups.

Atmaja is enrolled with the Delhi Bar Council and has a keen interest in academia. She has published articles on contemporary legal issues in reputed international and national journals and delivered lectures on intermediary liability at leading Indian law schools. In February 2022, Atmaja was recognised as one of the youngest Future Legal Leaders by *India Business Law Journal*.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

In the past year, India has taken significant strides in bolstering its cybersecurity standards, in order to ensure user safety on the internet. The regulators typically favour sectoral guidelines, in absence of any umbrella legislation.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were issued by the Ministry of Electronics and Information Technology (MeitY), in February 2021, which now provide users with a comprehensive grievance redressal mechanism, and further mandates intermediaries to assist government agencies in any investigation into any cybersecurity incident and provide information in their control within 72 hours of receipt of a government order.

As recently as April 2022, the Indian government's Computer Emergency Response Team (CERT-In) overhauled the breach reporting guidelines in India, by introducing directions in relation to information security practices, procedures, prevention, response and reporting of cyber incidents (CERT-In Directions, 2022). These directions, inter alia, mandate each body corporate to: (i) report cybersecurity incidents within six hours of notice to CERT-In; (ii) store system logs locally in India for all information and communications technology (ICT) systems for 180 days; and (iii) furnish information or any assistance if directed by CERT-In for the purpose of proactive and preventive actions relating to cyber incidents.

Further, the sectoral regulator Department of Telecommunications (DoT) has released a best practice guideline that provides guidance on safe computer practices, internet and email handling practices, avoiding social engineering attacks and safe methods of using digital signatures. To strengthen financial data management, in September 2021, the Reserve Bank of India (the nodal banking sector regulator in India) issued guidelines mandating tokenisation and masking the user's card details for all payments through online platforms, to secure user data.

Separately, the pending data privacy legislation (by way of its several iterations) may bring about further changes to this, by introducing sector-agnostic compliance and reporting requirements.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The aforementioned CERT-In Directions, 2022, mandate reporting of data breach incidents to a regulatory body (ie, CERT-In) within six hours of knowledge of any cybersecurity incident in their ecosystem. Failure to comply with the breach

reporting regime may invite punitive action, which may extend to imprisonment for up to a year, or a fine up to 100,000 rupees, or both. These directions provide for the types of cybersecurity incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and government organisations to CERT-In.

The banking regulator, the Reserve Bank of India (RBI), mandates that cyber incidents (including: (i) outage of critical IT systems; (ii) cybersecurity incidents; (iii) outage of infrastructure; and (iv) theft or loss of information) are reported to the RBI within a period of two to six hours.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

In the event of a data security incident, as a matter of practice, every company must prioritise: (i) using a prompt and accurate incident reporting mechanism, (ii) deploying resources for analysing the incident and its resultant impact; and (iii) finally adopting remedial measures so that a similar incident is not repeated.

Depending on the experience, the companies must ensure that their internal policies, reporting procedures and protocols are all aligned to meet the regulatory and compliance requirements.

A data security incident may also indicate a lapse in technical and organisational standards and the need to upgrade or develop the security standards. Continued evaluation of access controls (including physical access to protected systems), and scrutiny of measures in place through continuous and deliberate risk assessments, is necessary to maintain and upgrade security standards. Companies that are data fiduciaries should ensure that their obligations are mirrored with those of the data processors, to allow speedy reporting and compliance with early recovery protocols.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Entities operating in India are statutorily required to adopt reasonable security practices and procedures that are commensurate with the best industry practices, and that can be relied upon for the specific nature of datasets, and the applicable sector. Companies are increasingly relying upon international standards to improve their cybersecurity preparedness by the adoption of International Standard IS/ISO/IEC 27001 on Information Technology – Security Techniques – Information Security Management System Requirements. Owing to the extraterritorial applicability of GDPR, the Indian companies are already acting in compliance with practices so cited therein. Apart from this, with the host of service providers also having a marked presence across the US jurisdiction, they also comply with the state specific privacy, consumer data and child protection legislation.

Indian organisations are cognisant of their responsibility, and in this regard they also conduct regular data protection impact assessments (DPIA), deploy security information and event management systems (SIEM) for real-time monitoring and analysis of events, tracking and logging of security data for compliance or auditing purposes, so that potential security threats may be recognised and dealt with adequately without any business disruption.

Implementation of security safeguards may include the adoption of encryption, de-identification measures such as hashing, anonymisation and two-factor verification to ensure the confidentiality and integrity of the data. With increased incidence of work from home, companies are relying on use of virtual private networks, and deployment of data servers at an enterprise level for the purposes of effecting robust cybersecurity frameworks. With cloud service providers also offering advance solutions, it is not difficult for companies to adapt to the better security practices.

> "Implementation of security safeguards may include the adoption of encryption, de-identification measures such as hashing, anonymisation and two-factor verification to ensure the confidentiality and integrity of the data."

Further, deployment and implementation of standard protocols for employee training, in security principles and safe data handling measures arm the processors of the information with the relevant safeguards, obligations to ensure data subject rights are not eroded. Limited access to data, restrictions upon accessing 'not safe for work' websites and such other measures are also routinely streamlined. For instance, certain employers do not even allow the WhatsApp web, iCloud and Google Drive to be accessed from the company devices, to ensure that no information is breached or compromised or tampered with owing to unwarranted access being provisioned within their own devices.

5 | Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

It is of paramount importance that businesses planning to move data to a cloud hosting environment must first consider the legal implications, and compliance requirements, of the transfer in accordance with the sectoral regulations on outsourcing data processing, data localisation norms and other requirements.

Photo: shutterstock.com/Mikadun

Further, cross-border transfer of data will necessitate adherence to transfer regulations of foreign jurisdictions, which may be required with that particular recipient nation-state. It is important for the engaging businesses to evaluate the locations from which the CSPs operate, the measures that are in place and the standards that they adhere to, in order to be compliant with the data localisation norms (if any), and to be effectively deploy business continuity and disaster recovery measures.

In the absence of any law lending specific guidance on engaging CSPs for work of this nature, businesses must execute a well-negotiated contract with the external vendors to ensure that the performance and offerings of the CSP corresponds with the requirements of the business and the laws of the land.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

As indicated in question 1, in the past year, the Indian government has brought about a remarkable regulatory overhaul to address cybersecurity incidents. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code)

Rules, 2021 and the CERT-In Directions, 2022 have strengthened cybersecurity preparedness by advocating and mandating expeditious reporting and investigation into cybersecurity incidents. The Information Technology Act 2000, read with extant regulations, penalises cybercrimes, making the offenders liable to imprisonment or fines, or both.

The government is evaluating serious cybersecurity threats and even banned malicious websites and applications by invoking the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, as a pre-emptive measure to prevent cybersecurity incidents. The Indian government also engages in constant dialogue with stakeholders, inviting comments on relevant issues concerning cybersecurity and data protection prior to introducing any new regulatory measure. The pending data privacy legislation is being deliberated upon further with respect to inclusion of aspects concerning the security of non-personal data as well, which if enacted in its current form, will further strengthen the security standards to be adopted by organisations. The government is also contemplating the adoption of a National Cybersecurity Strategy to adequately address increasing cybersecurity incidents.

In addition, the CERT-In conducts regular assessments and investigations, uploads publicly accessible reports addressing current cybersecurity concerns, forecasts and alerts cybersecurity incidents, coordinates cyber incident response activities and issues advisories and guidelines on prevention, response and reporting of cybersecurity incidents. Additionally, other sectoral regulators also independently and proactively evaluate the standards necessary or typical in their sectors. With these CERT-IN Directions, 2022, there has been a commitment that with reporting of the incidents and log reports being submitted to the authority, the CERT-IN would also share reports with the larger group for their consumption and better understanding of how things might work better at an implementational level.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

While contemplating M&A deals, companies must undertake thorough due diligence of the existing company posture on data privacy and security. There must be thorough investigation of the internal policies, protocols, vendor engagement and management, on the part of the 'acquired company'. In the event of transitioning or integration of any software or online environments of the two companies, there must be a data protection impact assessment conducted right at the start. It is not ideal for the companies to merge their datasets at the first instance, but to let the consolidation take place only upon subsequent evaluation of the policies as well as

the protocols followed by both the companies. The companies should be aware of the fact that there could be a difference even at a basic cultural level, in both the entities, and this can only be dealt with in a gradual process.

The companies must ensure that the policies of both the entities can be aligned to come from a single source of truth. There will have to a structural change in the organisational structure and hierarchy that governs access to the personal data available within the entity. This will also lead to changes in the third-party services that may be engaged by either party, to be able to bring in parity. Furthermore, the entities must also familiarise themselves with any peculiar sectoral compliance requirements, or that of a particular jurisdiction, or a registering authority (for cross-border transactions, some jurisdictions might have registration requirements), as the case may be.

Abhishek Malhotra
amalhotra@tmtlaw.co.in

Atmaja Tripathy
atmaja.tripathy@tmtlaw.co.in

TMT Law Practice
New Delhi, Mumbai and Bangalore
www.tmtlaw.co.in

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Clients should seek legal counsel from lawyers with technical knowledge along with appropriate sectoral knowledge. It is advisable to choose a one-shop stop where lawyers can assist with legal compliances in the relevant sector as well structure advice factoring in concerns that may arise at the stage of dispute resolution. Lawyers should be abreast of the latest cybersecurity threats/incidents and the technological and organisational standards adopted to address such threats.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

The absence of a central data protection law that adequately addresses data security and breach issues, along with the ambiguity from amendments to the pending data privacy legislation, complicates the advisory work. Sectoral rules make it challenging to assume compliance for an entity with diverse business activities.

How is the privacy landscape changing in your jurisdiction?

The privacy landscape in India is undergoing a slow yet substantial change. The pending privacy legislation has undergone several amendments. The last iteration underwent a complete overhaul with introduction of non-personal data into the fold. The judiciary's proactive measures, starting with the right to privacy as a constitutional and fundamental right, have led to constitutional courts now recognising an individual's right to be forgotten as an offshoot of the right to privacy.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

Server access and system attacks, cloud attacks, data theft, impersonation, mail-spams, fake applications, ransomware and malware are the most common cybersecurity incidents in India. The CERT-In Directions, 2022 identify approximately 20 types of cybersecurity incidents. Companies should be mindful of this list for reporting and investigation protocols, and adopt appropriate technological measures.

Italy

ICT Legal Consulting is an international law firm founded in 2011 with offices in Milan, Rome, Bologna, Amsterdam, Athens, Madrid, Helsinki and Melbourne, and a presence in 49 other countries: Albania, Austria, Bangladesh, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, China, the Czech Republic, Denmark, France, Germany, Ghana, Hungary, India, Indonesia, Ireland, Israel, Japan, Kenya, Luxembourg, Mexico, Moldova, Montenegro, New Zealand, Nigeria, North Macedonia, Norway,the Philippines, Poland, Portugal, Romania, Russia, Serbia, Singapore, Slovakia, South Africa, South Korea, Sweden, Switzerland, Taiwan, Thailand, Turkey, the UAE, Uganda, the UK, the US and Vietnam.

ICT Legal Consulting was established in 2011 by Paolo Balboni and Luca Bolognini, who have successfully assembled a network of trusted, highly skilled lawyers specialising in the fields of information and communication technology, privacy, data protection/security and intellectual property law.

ICT Legal Consulting's highly skilled lawyers advise companies and businesses, including multinationals, on legal, ethical and technological issues in the areas of privacy, data protection, and data valorisation, digital rights, IoT, AI, TMT, IP, data governance and integrated compliance models offering a strategic and holistic approach to turn legal advice into a competitive advantage for clients.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

In recent years, we have witnessed the creation of a body of legislation that is as innovative as it is admirable, aimed at protecting the activities of the state entity. In particular, the first piece at the European level is represented by Directive (EU) 2016 2016/1148 of 6 July 2016 on network and information security (the NIS Directive), implemented in Italy through Legislative Decree No. 65 of 18 May 2018, which was followed by Decree-Law No. 105 of 2019 (converted and amended by Law No. 133 of 18 November 2019) that formally established a National Cybersecurity Perimeter (PNSC). It aims to ensure a high level of security for networks, information systems and IT services of both the public administration and national, public and private services, entities and operators. Subsequently, in implementation of Decree Law No. 105 mentioned above, Prime Ministerial Decree No. 131 of 30 July 2020 provided the criteria for identifying the subjects included in the PNSC and the related obligations from the point of view of national security protection. Among the subjects that are part of it, we find the operators of the various sectors (eg, space and aerospace, energy, telecommunications, transport, digital services, health and social security institutions), which will have to indicate in advance the ICT assets that they consider necessary to carry out the activities described above, in order to ensure the integrity, efficiency and security of data and all the information they process. In this sense, the subjects included in the Perimeter will have to carry out various activities, such as – by way of example but not limited to – the annual updating of the lists of their ICT assets, the risk assessments aimed at identifying risk factors (precisely) and the management and implementation of the necessary security measures.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

A security breach may result in the destruction, loss, modification, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. It may occur unlawfully or accidentally and may compromise the confidentiality, integrity or availability of personal data. For example, we speak of access to personal data when the following events occur (even simultaneously and cumulatively): access or acquisition of data by unauthorised third parties; theft or loss of computer devices containing personal data; loss or destruction of personal data due to accidents; and unauthorised disclosure of personal data. The data controller – whether it is a public entity, a company, an association, and so on – must notify the breach

Francesco Capparelli

Serena Pistritto

Andrea Sudano

Francesca Tugnoli

to the Italian Data Protection Authority for the protection of personal data without undue delay and, where possible, within 72 hours of the moment it became aware of it. Similarly, the data processor who becomes aware of a possible violation must promptly inform the data controller, so that the latter can take action. It should also be noted that the notification made to the Italian Data Protection Authority after the deadline of 72 hours must be accompanied by the reasons for the delay. Finally, the violation of personal data must be communicated to the persons concerned if it may involve a high risk for the rights and freedoms of individuals. It should be borne in mind that, independently of the notification to the Italian Data Protection Authority, the owner or the person in charge of the processing are required to document all violations by means of a special register, in order to allow the performance of any verification activities by the Authority in accordance with the regulations.

However, in terms of assessment, the impact of the data violation is related to the nature of the data breached. If the breach concerns sensitive data (such as, for example, financial information, or data relating to health, religious or political orientation), it is highly likely that this will involve a risk for those concerned. On the other hand, a breach involving only general information (such as, for example, name,

Photo: shutterstock.com/cge2010

surname and email address) is less likely to pose a risk to data subjects. Moreover, always in optics of evaluation, it is necessary to verify if as a consequence of the violation physical persons can suffer a physical, material or immaterial damage. The occurrence of a personal data breach, especially a sensitive one, may generate impacts of a discriminatory, reputational or financial nature. Therefore, this assessment must be carried out individually for each incident, as – depending on the concrete case – seemingly similar breaches may lead to very different outcomes.

In this sense, the Recommendations provided by ENISA offer valuable support in identifying a methodology for assessing personal data breaches. Furthermore, the Guidelines provided by the European Data Protection Board (EDPB) not only represent a collection of examples of notifications received over the years, but also provide support for data controllers throughout the entire process (ie, from the initial assessment of the risk and the related threat to the evaluation of preventive measures and, finally, the occurrence of the incident).

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

The effects that can derive from a security incident are multiple and vary according to the type of organisation that has suffered the attack, the data violated and the ability to manage the incident. In order to mitigate the impacts that may result from an incident, it is of fundamental importance to equip the organisation with technical and organisational measures aimed at mitigating the incident. From an organisational perspective, an IT security incident response plan must be prepared, documented and regularly updated, including the activation of relevant functions for proper and efficient incident management. This gives you a better chance of mitigating any associated risks and limiting the impact of the incident. In addition, the presence of an effective incident management plan ensures a greater ability for the organisation to continue its 'critical' activities and thus ensure business continuity without impacting its reputation. On the other hand, from a technical point of view, the organisation should implement incident detection solutions, such as, for example, the use of a SIEM (security information and event management) or a SOC (security operations centre). In the first case, this is a system that centrally collects logs and events generated by networked applications and systems, allowing security analysts to reduce the time required to resolve and investigate security alerts and incidents. In the second case, however, the SOC is nothing more than a structure in which all information about the security status of the IT of one or more companies is centralised (in this case, the SOC belongs to a managed security service provider, MSSP).

In addition, it is essential that clear roles, tasks and deadlines are assigned to each manager and that these are formally set out in a procedure. A key role is also played by the emergency response team, whose task is, first, to assess the incident and ascertain whether it should be considered a data breach. Next, if the incident consists of a data breach, the organisation will need to verify whether, under article 33 of the GDPR, the incident should be notified to the Authority and the data subjects whose data was breached. To best perform this activity, it is advisable for the organisation to have both a data breach assessment unit and a data breach management unit. It should also be pointed out that the risk could be made public even if the event does not have to be communicated to the data subjects, for example, if a firm suffers a phishing attack from a hacker. This could result in both an economic impact on the organisation – caused by the imposition of fines on the organisation – and a reputational impact that could also lead to contractual losses with partners and suppliers.

As such, we advise our clients to maintain a proactive approach to data breach communication. It is precisely for this reason that many companies decide to inform data subjects of a breach, despite the fact that it is not legally required by the GDPR. In this way, the organisation demonstrates to its customers that it is taking all necessary measures, generating a relationship of trust with them. It is crucial for organisations not to underestimate the impact of a data breach and be perceived as trustworthy by their customers. This can be achieved by implementing all appropriate technical and organisational measures, including the introduction of staff training to minimise the risk of human error. Finally, if the incident has been caused by an intentional action, it is advisable to report the incident to the police, in order to avoid possible accusations of complicity or co-responsibility with the attackers.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

One of the most important security measures followed by organisations is the scheduling of training courses for personnel. The aim is, on the one hand, increasing the level of preparation and awareness of their employees, and, on the other hand, preventing human error. Human error represents one of the highest risks for company personnel if not subjected to continuous training. Therefore, training should cover both the main threats to cybersecurity and the behavioural norms that must be adhered to in order to limit those threats. Digital platforms are the best solution for conducting targeted courses (eg, webinars, training events, tests and, in general, all training activities) aimed at increasing staff awareness through theoretical notions and practical activities (eg, final learning tests) on cybersecurity

> "Human error represents one of the highest risks for company personnel if not subjected to continuous training."

and privacy issues. Another security measure is the formalisation of the best practices adopted by organisations, in compliance with the main international standards on privacy and cybersecurity, through the presence of appropriate policies and procedures. Finally, the implementation of adequate controls on human resources is also a valid security measure, aimed at reducing the probability of accidental or malicious threats, for example, background and competency checks on all candidates for employment.

5 | Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

The increasing use of the cloud for information storage has increased the focus on protecting the data it contains. In particular, the security of such information becomes essential in the case of clouds that store personal data. In this context, there are two international standards of reference, namely, the ISO 27017 standard and the ISO 27018 standard. These two standards extend the controls of ISO/IEC 27001 and introduce specific additional controls.

Specifically, ISO 27017 'Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services' defines general security controls for both cloud service providers and their customers.

ISO 27018 'Code of Conduct for the Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Managers' is a code of conduct for cloud providers that focuses on the protection of personally identifiable information (PII) in public cloud services, constituting guidelines for cloud providers acting as data controllers. Both standards should be integrated into ISO 27001 certification when the scope includes cloud services. They also imply the need for specific training on the cloud, particularly its critical aspects and the management of related access rights. Training, therefore, should be targeted at administrators, users, employees and third parties.

When moving to a cloud hosting environment, it is also essential to ensure business continuity, as regulated by ISO 22301 'Societal security – Business Continuity Management Systems – Requirement'. This standard concerns the construction and continuous improvement of the level of business resilience. Specifically, it defines the requirements necessary for the planning, implementation and monitoring of

Photo: shutterstock.com/VividaPhotoPC

a documented management system, aimed at the continuous improvement of the management system. In particular, compliance with this standard ensures not only greater protection of the organisation's information, thereby reducing the likelihood of business or security incidents, but also optimises response times and recovery activities following a security incident.

In addition to these, there is also the ANSI/TIA-942 standard for data centre protection. The American National Standards Institute (ANSI) is a body that certifies the guidelines on how infrastructures must be built; while the Telecommunications Industry Association (TIA) is an ANSI-accredited association created to voluntarily develop standards based on the consensus of organisations for a wide variety of ICT products.

In this regard, there are two other codes of conduct for personal data protection and cloud computing to refer to, which have been endorsed by the EDPB for personal data protection and cloud computing: the EU Cloud Code and the Cloud Infrastructure Service Providers Code.

In accordance with the above, organisations should perform a number of checks and evaluations against cloud solution providers. First, they should verify the technical and organisational security measures offered by the cloud solution provider and pay particular attention to the location of data centres. This is also relevant by virtue of the fact that many cloud providers use data centres located in different countries, even outside the European Economic Area, as indicated by article 46 of the GDPR, which provides appropriate safeguard clauses for this type of transfer aimed at data protection. Moreover, when a company relies on a cloud provider, it should ensure the legitimacy of the data transfer, also in light of the requirements established by the European Court of Justice – following the well-known *Schrems II* judgment – and the recommendations provided by the EDPB. Finally, the customer who relies on the cloud service provider should carry out an assessment of the risks arising from the transfer of data, calculating the likelihood of that risk occurring and the impacts it could generate. In this assessment, it is necessary, therefore, to analyse the security measures implemented by the provider aimed at limiting the impacts, as well as the additional security measures to be implemented aimed at mitigating any impacts. Such an assessment is necessary because, according to the recommendations provided by the EDPB and in accordance with the *Schrems II* judgment, if the security measures envisaged are not adopted or are adopted only in part, so as to be insufficient, the transfer should be suspended, or the competent supervisory authority should be notified.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The Italian government has set up an Italian national police unit that aims to conduct investigations into cybercrimes and cyberterrorism and the protection of critical national infrastructure. Moreover, with Legislative Decree 65/2018, the Italian Computer Security Incident Response Team (CSIRT) was established within the Department for Information Security of the Presidency of the Council of Ministers, whose mandate is to monitor incidents at the national level. Also, part of the CSIRT network is a network composed of CSIRTs appointed by EU member states. Further tasks of the CSIRT concern the issuing of early warnings, alerts and announcements, the dissemination of information to interested parties on risks and incidents and, above all, the intervention in the case of cybersecurity incidents. With regard to the computer crimes punished within the Italian criminal law, we find lots of crime punished by the Penal Code. For example, abusive access to computer systems, damage to computer systems and computer fraud, respectively under articles 615-ter, 635-bis and 635-quater, and 640-ter of the Penal Code. These are regulations can be committed by anyone and cover most of all the action can committed by informatic instruments. Those crimes have severe punishment if committed by someone that can be qualified as system administrator and become prosecutable *ex officio*. Recently, the Italian Supreme Court interpreted digital documents as an asset having content susceptible to apprehension and capable of integrating the case of theft punished by article 624 of the Penal Code. In the Italian criminal legislative landscape, the computer crimes mentioned above are also relevant under the provision of Legislative Decree 231/2001, article 24-bis. This means that if those crimes are committed on behalf of the legal entity, the company will be responsible for those crimes.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

In the evaluation that companies put in place during M&A transactions, one of the most important aspects to take into account relates to the level of IT risk of the target organisation and the security measures of the latter, placed to protect its information assets. In this sense, it is good to talk about data protection compliance and cybersecurity due diligence. In fact, it is good to underline how accurate compliance with privacy and a careful protection of data and its quality, which can influence the actual value of the databases and information resources of the target organisation, are fundamental evaluation parameters. As an example, consider the fact that a

> "If consent of data subjects has not been properly provided, there is a serious risk that the entire data set will be unusable and need to be deleted."

large database of clients or potential clients can be a valuable resource that carries weight in negotiations, but if the database has not been developed in full compliance with all the provisions of privacy law (for example, if consent of data subjects has not been properly provided), there is a serious risk that the entire data set will be unusable and need to be deleted. Concomitantly, the security risk-based approach should also be taken to objectively determine and assess cybersecurity threat scenarios that could impact the target organisation, accompanied by the likelihood of their occurrence and potential impact. In fact, as a first step, an assessment should be made that includes all aspects that have a major impact on the business and the potential threats that could affect the stakeholders, before, during and after the M&A process. In particular, the cyber governance of the target organisation should be assessed, considering the technical and organisational measures implemented, the resources employed and the level of corporate awareness. In this regard, it is of fundamental importance to verify that the target organisation conducts regular training on privacy and cybersecurity aspects and that it implements internal security measures aimed at certifying the effectiveness and efficiency with which all cybersecurity-related activities are conducted. Here are a few examples: software and firmware updates, review of authorisation profiles, firewall rules and other

configurations, management of an inventory of resources, prevention and detection of possible attacks both from outside and inside organisational environments and management of incident response and recovery activities.

Quantifying the value of all the target organisation's information assets (for example, if these assets are part of the core business), is also important for assessing the impact of potential security incidents. This impact sometimes depends on the type of technology platforms used by the target organisation (eg, cloud, on-site, physical machines or virtual machines, choice of operating systems and databases) and, consequently, the security measures implemented.

Finally, consideration should be given to whether the target organisation has (third-party) vendors. If so, it is prudent to conduct an assessment of the security measures implemented by those vendors within their organisation and in relation to the service/product offered to the target organisation, through second-party audits of each vendor's technical and organisational infrastructure.

Francesco Capparelli
francesco.capparelli@ictlc.com

Serena Pistritto
serena.pistritto@ictlc.com

Andrea Sudano
andrea.sudano@ictlc.com

Francesca Tugnoli
francesca.tugnoli@ictlc.com

ICT Legal Consulting
Milan, Rome, Bologna, Amsterdam, Athens, Madrid, Helsinki and Melbourne
www.ictlegalconsulting.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

With the accelerated growth of the digital security market, the demand for competent and up-to-date cybersecurity specialists is increasing. This type of consultancy requires continuous professional training , multidisciplinary skills in privacy, a good knowledge of how technology works and good communication skills.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

The GDPR requires organisations to comply with the principle of accountability, implementing all appropriate technical and organisational measures to ensure – and demonstrate – that data processing is carried out in accordance with this Regulation. Data protection has taken on a central role, and the development of new technologies must be carried out in compliance with international standards and the GDPR, with a view to privacy by design and privacy by default, namely right from the design phase.

How is the privacy landscape changing in your jurisdiction?

The Italian landscape in the field of privacy has undergone an enormous evolution with the introduction of the GDPR first, and then with the ePrivacy Regulation. Therefore, important challenges have been posed for a variety of organisational realities, both public and private in terms of personal data protection. However, the EU privacy rules will have finally completed their modernisation process.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

The Clusit Report 2022 – March 2022 Edition shows that global attacks increased by 10 per cent compared to the previous year, and that these attacks are more serious. In particular, attacks towards Europe have grown to 21 per cent of the total, up from 16 per cent in the previous year. Cybercriminals are no longer hitting multiple targets, but very specific targets. A large portion of data breaches also occurs due to human error, which be mitigated through staff training.

Japan

Tetsuya Oi, a partner at TMI Associates, is well versed in professional practices in various industrial fields, including the protection of personal information, EU data protection regulations, information security cloud services, internet content, internet of things, artificial intelligence, advertising technology and development of system applications.

Satoshi Murakami, a partner at TMI Associates, specialises in data protection, intellectual property law, internet-related law and consumer-related laws, among other fields. In particular, he has continuously represented and advised numerous domestic and international companies primarily in the technology, telecommunications, video game, e-sports, media and e-commerce industries.

Shunsuke Terakado, a partner at TMI Associates, specialises in data protection, cybersecurity, IT transactions, technology disputes involving massive data breaches, system integration projects and IP licensing. He is a Registered Information Security Specialist (the national qualification in cybersecurity) and provides advice based on both his legal and his technological knowledge.

Shohei Suzuki, an associate at TMI Associates, specialises in privacy and security law and other internet-related laws, as well as mergers and acquisitions. He has substantial experience in privacy issues relating to advertising technology and acquisitions of companies holding personal data of internet users. He is licensed to practise in both Japan and California.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

The cybersecurity requirements applicable to most companies operating in Japan are those stipulated in the Act on the Protection of Personal Information (APPI). The APPI requires companies to take necessary and proper measures to prevent leakage, loss or damage of personal data, and to provide other security control of personal data. Guidelines issued by the Personal Information Protection Commission (PPC) explain what companies should do in order to comply with the requirements of such measures. According to the guidelines, a company is required to implement organisational, personnel, physical and technical security control measures. The guidelines make it clear that appropriate security control measures can differ from company to company, so a company should determine its appropriate security control measures while considering expected impacts on the rights and interests of data subjects in the case of data breaches as well as the possibility of data breaches.

The June 2020 amendments to the APPI, which include several important changes, came into full effect on 1 April 2022. With regard to cybersecurity requirements, the following three changes should be noted.

First, the penalty for the failure to implement appropriate security control measures has been strengthened. Under the Act prior to the amendments, a company that receives a corrective order from the PPC for failing to take appropriate security control measures and then fails to obey that order could be subject to a fine of up to ¥300,000. However, under the amended law, the upper limit of the fine is ¥100 million, and officers and employees who fail to obey the order can also be subject to a fine of up to ¥1 million or imprisonment for up to one year.

Second, under the amended Act, businesses are legally obligated to report data breaches meeting the thresholds to the government and the data subjects.

Lastly, the amended Act requires a company to make the information about the security controls taken by the company available to data subjects. Companies may choose either making the information public (eg, posting a privacy policy containing the information on its home page) or providing the information to a data subject at their request. The information to be offered includes the names of the countries in which personal data is stored.

Another relevant act is the Basic Act on Cybersecurity, the purpose of which is to move cybersecurity-related policies forward in a comprehensive and effective manner and to contribute to the creation of a more energetic and continuously developing economic society, thereby contributing to the national security of Japan. This Act mainly stipulates the basic principles of Japan's national cybersecurity


Tetsuya Oi


Satoshi Murakami


Shohei Suzuki


Shunsuke Terakado

policy and the responsibilities of the national government, local governments and other concerned public parties. It requires businesses to make voluntary and proactive efforts to ensure cybersecurity, but there is no penalty for failing to fulfil this requirement.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

As mentioned in question 1, the 2020 amendment to the APPI came into full effect on 1 April 2022. The amended APPI requires businesses to report breaches of personal data to the PPC and affected data subjects when the data breaches involve actual or possible breach:

- of sensitive personal data;
- of personal data where unauthorised use of the data is likely to cause financial damage;
- that may have been caused with a malicious purpose; or
- where more than 1,000 data subjects are affected.

A 'data breach' here includes not only leakage of personal data, but also loss of and damage to personal data.

A business must promptly (ie, within around three to five days) notify the PPC once a data breach comes to their notice. Furthermore, the business must file a complete report to the PPC within 30 days or, if the data breach is likely to have been caused with a malicious purpose, within 60 days. Both reports must be made online through the PPC website by submitting a report form available on the same website.

Notices to the affected data subjects also need to be made in a timely manner depending on the situation after the business comes to know of the data breach. Businesses will be exempted from this reporting requirement if there is a situation that makes the reporting to the data subjects difficult and the business takes substitute methods to protect their rights and interests. For example, if a business does not have contact information of the affected data subjects, it does not need to provide notices to them but must publish the fact of the data breach and respond to inquiries from the data subjects.

When a company handles personal data on behalf of another entity under an entrustment agreement, both parties are subject to the notice obligation upon the event of a data breach. However, the entrusted party will be exempted from the obligation if it reports the data breach to the entrusting party.

In addition, a report is not required in the following cases:

> "Under the amended Act on the Protection of Personal Information, businesses are legally obligated to report data breaches meeting the thresholds to the government and the data subjects."

- an advanced encryption method is adopted for the leaked information;
- all the leaked information is recovered before a third party can view it; or
- the business has a complete copy of the personal data that was lost or damaged.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

When suffering a data security incident, the main issues that companies need to address from a privacy perspective are conducting a prompt and appropriate incident response, and ensuring accountability and transparency to data subjects and other stakeholders.

While companies have been increasing their use of data, such as by acquiring and analysing internet browsing history and location data for marketing purposes, major data security incidents attracting public attention have occurred in Japan in recent times. For example, there was unauthorised access to a mobile payment service and the service was scrapped just one month after its debut as the company struggled to resolve the security issues and restore the trust of its users. This

incident reaffirmed that data breaches can have a significant impact on businesses and that preparing for incident response including accountability and transparency to data subjects is extremely important for business continuity.

Although the incident response procedure and security measures to be taken by companies may vary depending on the individual data security incident, there are a number of procedures that are usually recommended in the event of a data security incident, to prevent the spread of damage and ensure transparency and accountability to data subjects and other stakeholders.

First, immediately verify the facts concerned, including the causes of the data security incident and the scope of data that has been leaked. Then, immediately announce the accurate facts and express sincere apologies to data subjects – do this at an early stage, as a first and quick announcement. Immediately make a first quick report to the PPC and other related authorities depending on which industry the company belongs to. Next, continuously announce and report to data subjects and the relevant authorities the facts that may be revealed from subsequent investigations. Perform investigations, including digital forensics, conducted not only by internal members, but also by a third-party committee consisting of specialists

Photo: shutterstock.com/SeanPavone

(including attorneys and technical specialists) who are in neutral positions to perform investigations. Security management measures must be planned based on the results of the investigations performed, to prevent any recurrence of the data security incident. Finally, the company must report the results of the investigations performed and the security management measures to prevent any recurrence of the data security incident, and it must implement the security management measures.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

There is no single best practice to improve cybersecurity preparedness for all businesses in Japan. Generally, the security management measures to be taken by companies should be determined through self-assessment taking a risk-based approach. Accordingly, it is important to duly carry out certain processes for improving cybersecurity preparedness:

- collect the latest cybersecurity-related information and trends;
- figure out the current status of the company's security management measures;
- carry out a risk assessment and establish security management measures in accordance with the results of the assessment; and
- operate appropriately.

Since there are laws, regulations and guidelines providing a baseline that can help companies to conduct this type of assessment, we will consider them to provide an example here.

First, as we mentioned earlier, the APPI requires companies to take necessary and proper measures to prevent the leakage, loss or damage of personal data and to provide other security controls for personal data. The guidelines issued by the PPC explain what companies should do to comply with these measures. According to such guidelines, a company is required to implement organisational, personnel, physical and technical security control measures. In addition, the amended APPI requires companies to make the information about their security measures available to data subjects. Furthermore, the Financial Services Agency has issued additional guidelines that stipulate matters that require companies in the financial sector to take particularly strict security control measures in light of the nature and use of personal data in the financial sector.

Second, the Ministry of Economy, Trade and Industry has published the Cybersecurity Management Guidelines that are intended for companies that are utilising IT-related systems or services. The guidelines describe managerial strategies from the perspective of protecting companies from cyberattacks and

recommend companies to implement security management measures that are based on three principles that the manager of a company should be aware of and 10 significant items that a manager of a company should instruct to the officer responsible for executing information security measures (eg, the chief information security officer who is in charge of supervising information security within the company).

Third, the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) operates an assessment system for certifying whether or not the information security management system (ISMS) of a company is consistent with international standards (the ISMS conformity assessment system). Under this assessment system, examinations are made as to whether or not an ISMS implemented by a company is in conformity with JIS Q 27001 (ISO/IEC 27001). In addition, the JIPDEC also operates a PrivacyMark System to assess companies that take appropriate measures to protect personal data.

Fourth, the Centre for Financial Industry Information Systems (FISC) has established the 'FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions' to promote security measures on financial institution information systems. These guidelines have been voluntarily observed by most financial institutions in Japan.

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

Cloud hosting services are currently in use in a wide variety of situations in Japan. However, there are some points that should be considered by business operators upon using cloud hosting services.

The APPI regulates the transfer of personal data to third parties in countries outside Japan. Many of the cloud hosting services that are widely used in Japan are operated by service providers in foreign countries. If a foreign cloud service provider processes personal data in the cloud (ie, the cloud service provider accesses personal data managed by a user, a business operator in Japan and extracts some data linked with such personal data), then the user is subject to personal data transfer regulations. Under the APPI, if personal data is transferred to a third party in a country outside Japan, the transferring party is generally required to obtain the prior consent of the relevant individual for such cross-border transfer. However, it is not practicable to obtain consent from the individuals upon using a cloud service.

One of the exceptions that is widely used is where the third party is located in a foreign country that the PPC determines and prescribes by its rules as providing an equivalent level of protection of personal data as Japan (which is currently only the European Economic Area and the United Kingdom). Another exception is where

"If a buyer acquires a target company, the buyer will need to check whether it can use the target company's data after the acquisition."

the relevant third party has established, and continues to utilise, an equivalent level of protective measures as those that are required under the APPI, which can be met by entering into appropriate agreements between the user and the cloud service provider.

Thus, in cases where the cloud service provider processes personal data in the cloud, the provider must process such personal data in Japan or meet one of the above exceptions.

In addition, in cases where the cloud service provider processes the personal data in the cloud, the user shall supervise the processing of personal data by the cloud service provider. Thus, upon choosing a cloud service, the user needs to validate the appropriateness and security of the cloud service provider.

In contrast, if the cloud service provider and the user enter into an agreement whereby the provider undertakes not to access the personal data in the cloud, and the provider actually limits the accessibility of the personal data, the provider is not regarded as processing the personal data in the cloud and is therefore not subject to the personal data transfer regulations. Note, however, that the user is fully liable for any incidents in the cloud in this case. Thus, it is important for users of cloud

Photo: shutterstock.com/Phattanastock

services to validate the appropriateness and security of the cloud service provider in this case as well.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The increasingly established nature of technologies in cyberspace, such as AI, the internet of things, fintech, robotics, 3D printers, and AR and VR, has seen the expansion of cybersecurity threats.

The Basic Act on Cybersecurity enacted in 2014 provides for the basic policy for cybersecurity. Under the act, the government provides its Cybersecurity Strategy (the latest of which was made in 2021). The strategy shows the basic position and vision on cybersecurity, and objectives and implementation policies for the coming three years.

The Cybersecurity Strategy states that cybersecurity must be ensured for all people, business sectors, local regions, etc, and, in response to digitalisation, Japan will aim at ensuring cybersecurity 'with no one left behind'. Japan will continue to push forward with measures to ensure 'a free, fair and secure cyberspace' in an increasingly uncertain environment based on the following three approaches.

Simultaneously advancing DX and cybersecurity

The covid-19 pandemic and the establishment of the Digital Agency in September 2021 accelerated the digitalisation of the economy and society in Japan. Japan will continue to promote digitalisation along with efforts to ensure cybersecurity.

Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

Japan will deepen and enhance the approaches taken in the previous cybersecurity strategy formulated in 2018 (ie, it will deepen mission assurance and enhance efforts related to risk management) and work to improve the environment and address the causes of cybersecurity threats.

Enhancing Initiatives from the perspective of national security

Japan will strengthen its defence capabilities by securing the nation's resilience through the enhanced capabilities of the relevant government institutions. At the same time, Japan will enhance its deterrence capabilities to detect, investigate, and analyse cyberattacks so that Japan can identify the attackers and hold them accountable.

"The Cybersecurity Strategy states that cybersecurity must be ensured for all people, business sectors, local regions, etc, and, in response to digitalisation, Japan will aim at ensuring cybersecurity 'with no one left behind'."

In addition, numerous laws impose criminal sanctions regarding cybersecurity threats. For example, the Act on Prohibition of Unauthorised Computer Access prohibits spoofing, security loophole attacks and phishing as unauthorised computer access. In addition, the Penal Code prohibits the unauthorised creation or provision of electromagnetic records of unauthorised commands that do not operate in accordance with other persons' intention or that act against their intention, typically computer viruses.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

What are the privacy and data security risks in mergers and acquisitions?

Legal due diligence should be performed in order to mitigate privacy and data security issues in mergers and acquisitions from the perspectives that:

- as the importance of data increases, buyers may engage in mergers and acquisitions in order to use the data held by the target company after the acquisition; and
- the need to perform legal due diligence from a data security perspective is high, and if the data held by the target company cannot be utilised after the acquisition, the purpose of the merger and acquisition will not be achieved.

What aspects of legal due diligence need to be performed?

The first aspect is how personal data held by the target company can be used after the acquisition. The second is whether the target company's data security system is sufficient. In addition, there may be cases where potential security risks remain at the target company.

What points should be checked in terms of use of data?

If a buyer acquires a target company because it perceives the data owned by the company as being valuable, the buyer will need to check whether it can use the target company's data after the acquisition.

For example, when a food manufacturer acquires a company that operates a recipe website, the question is whether the food manufacturer can use the personal data of users visiting the recipe site. In this case, the legal due diligence should include checks to find out whether the personal data held by the target company is lawfully collected and whether the buyer can use the personal data held by the target company after the acquisition.

As regards the latter point, the question is whether the purposes of use after the acquisition are covered by the purposes of use held in the target's privacy policy

before the acquisition. If this is not the case, it is necessary to obtain consent from the users before using their data for new purposes.

What points should be checked in terms of data security?

Check whether the target company has established a security system for personal data and whether it has experienced any data breach incidents.

In particular, it is very important to check whether there are any potential data breach incidents and to have the seller represent and warrant that there have been no such incidents. If the buyer overlooks potential data breach incidents and also fails to obtain the representation and warranty from the seller, the buyer can be found solely responsible for incidents once they are revealed.

Tetsuya Oi
toi@tmi.gr.jp

Satoshi Murakami
smurakami@tmi.gr.jp

Shunsuke Terakado
sterakado@tmi.gr.jp

Shohei Suzuki
ssuzuki@tmi.gr.jp

TMI Associates
Tokyo
www.tmi.gr.jp

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Laws and regulations in the cybersecurity area include not only the APPI, but also the Unfair Competition Prevention Act, the Basic Act on Cybersecurity and other regulations and guidelines, and it is necessary to be familiar with all of these. However, often legal regulations alone are not enough to deal with actual cases. It is important for lawyers to be familiar with the latest threat information, security incidents from other companies and the technologies used to combat these, and to be able to give appropriate legal advice to clients.

How is the privacy landscape changing in your jurisdiction?

The APPI was amended in 2017, and this amendment introduced a rule that the APPI would be reviewed every three years as in the PDCA cycle. The PPC, which was established as an independent authority for data protection under the amendment in 2017, has issued administrative guidance and corrective instructions in some cases where it found inappropriate processing of personal data. In addition, the APPI was amended in June 2020 in accordance with the said cycle, with the amendments due to come into effect on 1 April 2022 , and under such amendment a monetary sanction was increased up to ¥100 million. We believe the regulatory environment for personal data will become stricter than it currently is, and businesses should be more cautious about data processing..

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

In Japan, companies need to be most careful of massive data breaches caused by advanced persistent threats (APT). Japan's Information Technology Promotion Agency (IPA) ranked APTs as the top threat in 2020 and the second top in 2021 and 2022. For their protection, companies must establish an organisational framework, develop a security policy, manage information and educate and train employees. They also need to be aware of security incidents caused by information leaks by internal fraudulent acts and compromised business email systems.


1674

Netherlands

Quinten Kroes heads Brinkhof's data protection practice and has been active as a lawyer in the telecommunications, media and technology (TMT) sectors since 1995, advising on and litigating matters of telecommunications, media and data protection law. He advises a broad range of companies on data protection. He has supported various companies that have been the subject of investigations by the Dutch Data Protection Authority.

Quinten's reputation is recognised as top tier in legal directories, as is the quality of Brinkhof's data protection practice.

Marije Rijsenbrij is an associate at Brinkhof and specialises in privacy and data protection. She advises clients on a broad range of data protection and cybersecurity-related issues.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

In terms of new legislation, several amendments and legislative proposals in the field of cybersecurity are noteworthy. In April 2022, a proposal to allow the National Cyber Security Centre (NCSC) to share information about cyber threats with the private sector in general, was submitted to the Dutch Lower Chamber of Parliament. The NCSC currently informs and advises vital providers and government bodies with up-to-date threat and incident information about their network and information systems. The proposal provides a legal basis to provide the same threat and incident information in certain instances to (private) companies as well. In March 2021, the Dutch government published a decree to designate which organisations qualify as 'operators of essential services' under the NIS Directive. This same decree also specifies what measures these operators should take to manage the risks to their network and information systems. The government used the opportunity to also amend the list of operators of vital services (a category that does not exist under the NIS Directive) but that are also subject to specific requirements under the Dutch act that implements the NIS Directive.

At the European level, the upcoming NIS 2 Directive will widen the scope of the current NIS Directive, covering medium-sized and large entities from more sectors than are covered by the current Directive and which are also considered critical for the economy and society at large. In May 2022, a political agreement was reached between the European Parliament and the Council. The agreement is still subject to formal approval. The European Commission also published a proposal for a Regulation on the European Health Data Space in May 2022. This has prompted the Dutch government to delay planning around its own proposal for the (Dutch) Act on Electronic Data Interchange in Healthcare. This proposal provides that healthcare providers may be required to exchange certain data in electronic form, provided that there is a legal basis for doing so (such as patient consent). Requirements can also be set for the technology to be used to exchange data, so that this exchange is not hampered by healthcare providers using different information systems. The Dutch DPA has been consulted and has expressed its concern that the proposal might force healthcare providers to breach their professional secrecy.

Aside from these new laws, the main regulatory development has been that the enforcement of the GDPR, both by the regulator and through collective class action claims, is really starting to take off. So far, the Dutch data protection authority's preferred method of enforcement seems to be the imposition of administrative fines. Cases where it has decided to impose an order or a ban on the processing of personal data, or issued a formal warning or reprimand, are the exception.

So far, the Dutch DPA has published 19 fines it imposed on both companies and government institutions for violating the GDPR. Three of these fines were imposed for a failure to notify a data breach in a timely manner and five fines for failing to implement sufficient security measures. Recently, the Dutch DPA imposed a fine of €525,000 on an online publisher for unnecessarily requesting copies of IDs from data subjects wishing to exercise their GDPR rights. Generally, the fines published by the Dutch DPA have been relatively high compared to fines imposed on average in other member states, although not near the level of the highest. In the past half year, the Dutch DPA imposed two record fines of €3.7 million and €2.75 million on the Dutch Tax Administration for illegally processing personal data in its fraud identification facility and for discriminatory and unlawful data processing respectively. Although both cases were quite unique and have also triggered a broader political and societal debate on racial profiling and discrimination, it shows that the Dutch DPA will not shy away from using its GDPR powers to go after the violation of other fundamental rights, such as the right to equal treatment. In concrete terms, it will take violations of other fundamental rights into account in determining the fine for the violation under the GDPR. The Dutch DPA has also imposed fines on relatively

> "The Dutch DPA has published 19 fines it imposed on both companies and government institutions for violating the GDPR."

small organisations, which are significantly lower than what its fining guidelines suggest. For example, an orthodontic practice was fined €12,000 for insufficiently securing the personal data that patients were uploading to its website. Similarly lower fines were imposed on a small foundation aligned to a Dutch political party, and an outdoor advertising company that had failed to adequately protect certain HR records.

Two of the fines that the Dutch DPA imposed have now been challenged in court. In the first case, which has attracted quite some media attention, the district court in Utrecht ruled that the Dutch DPA had wrongly rejected the 'legitimate interest' as basis for the processing of personal data by a company that offered amateur football clubs a platform to film and stream matches. In doing so, the court rejected the Dutch DPA's official position that purely commercial interests can never qualify as a 'legitimate interest'. The Dutch DPA has appealed this decision. In the other case, the district court in The Hague found that a fine on a local hospital was justified, but that the amount of €460,000 was unreasonably high. The court lowered it by €110,000, mainly because the hospital had taken a number of measures to prevent further violations.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

Pursuant to article 33 of the GDPR, a controller must notify a personal data breach to the Dutch DPA, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also, without undue delay, inform the data subjects, communicating in clear and plain language the nature of the personal data breach (article 34 GDPR). This communication is not required when the controller has taken measures to ensure that the risk of a breach is not likely to materialise. Breach notification requirements similar to those contained in the GDPR already existed in Dutch law since 2016.

Under the previous regime, the Dutch DPA had issued guidelines in English, which may continue to be useful for controllers who are confronted with a possible breach. The guidelines are, in some respects, more detailed than the guidance issued in 2017 by the Article 29 Working Party (WP 250), which was rather high-level and did not include very much practical guidance on how typical incidents should be assessed. This has now been remedied by the European Data Protection Board's (EDPB) new set of guidelines, adopted in December 2021, which offers concrete examples of the types of incidents that should be notified according to the data protection authorities.

All these documents make it clear that a number of criteria will be relevant to assess whether a notification needs to be made. These include the sensitivity of the data, the number of data subjects affected, the volume of data lost and the possible consequences for data subjects. Moreover, it is also considered relevant to take into account who received the information and to which categories of data subjects the data relate (eg, data relating to children or other vulnerable groups).

The Dutch DPA has also given further guidance on its website specifically on whether ransomware can qualify as a breach that needs to be notified. In short, it takes the position that this is indeed the case, as the illegal encryption of data implies illegal access to data and a circumvention of security measures that should have prevented this. The guidance issued in 2021 by the EDPB confirms this approach. The Dutch DPA also considers that it will often be hard to establish the precise effects of ransomware and to exclude the risk that it may have transferred or manipulated personal data in addition to encrypting the data. The Dutch DPA has recently stated that paying a ransom to (supposedly) prevent criminals from further spreading personal data after a ransomware attack, does not exempt organisations from notifying the personal data breach to Dutch DPA or data subjects. It does not

consider paying ransom an appropriate measure that will prevent high risks to the rights and freedoms of data subjects to materialise. After all, paying a ransom does not guarantee that hackers will actually delete (and not resell) all personal data.

In case of doubt, the Dutch DPA recommends to submit a preliminary notification of a possible breach. The notification can always be amended or even withdrawn at a later time, when the controller has more knowledge of the breach and its consequences. Controllers can notify through a web-based notification tool on the Dutch DPA's website, which was updated in 2021. Currently, this tool is only available in Dutch.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

Companies must continuously assess both the technical and the organisational measures they are taking to protect and secure their personal data. If a security incident occurs the company should give priority to fixing the particular security issue and do its utmost to mitigate the negative consequences of the breach.

Measures to be taken will vary depending on the type of incident, from trying to locate a lost data carrier, to contacting the recipients of an email that was wrongly sent or addressed, remote wiping of a portable device or working with a processor to establish the extent of a security incident in their domain. If a hacker may have obtained personal data, the company will have to assess whether or not the data had been sufficiently encrypted, as this is relevant to the question whether a notification should be made. If passwords have been leaked, the company should force users to change these passwords.

A data breach could be an indication that existing organisational and technical measures are not adequate. Maintaining appropriate and adequate levels of security requires continuous efforts and constant scrutiny through risk assessments, planning, executing, checking and doing the same all over again (the 'plan-do-act-check' cycle). The guidance adopted by the EDBP in 2020 on privacy-by-design and privacy-by-default confirms this. This is a logical consequence of the notion that the adequacy of measures must be viewed in light of current technical standards. It does not necessarily mean that, for example, technical measures need to be renewed at least annually to match the most advanced security system available. However, at least a suitable level of proactive monitoring is required: when imposing a fine on the Dutch Employee Insurance Agency (UWV) in July 2021, the Dutch DPA took into account the fact that the UWV did not sufficiently monitor and evaluate its security measures.

Photo: shutterstock.com/SAKhanPhotography

The strength of the measures should also be viewed in proportion to the nature of the data it protects. A pizza shop with a spreadsheet of local customer addresses for mailing promotional flyers will not need military-level encryption. But processing of sensitive data will require measures like two-factor authentication, encryption, hashing or, if possible, anonymisation or pseudonymisation.

The Dutch DPA considers two-factor authentication to be a common and fairly easy security measure to implement. Increasingly, organisations turn two-factor authentication on by default. According to the Dutch DPA, two-factor authentication is a minimum requirement for securing access to health data. Moreover, it should be borne in mind that the Dutch DPA not only considers the special categories of personal data as defined in the GDPR sensitive. In the past, it has recognised other categories of data, such as location data and data concerning someone's media consumption, as also sensitive in nature. Recently, the DPA imposed a fine on an airline company for not implementing strong passwords and two-factor authentication in its back office systems, which lead to a data breach.

Organisational measures to be applied include confidentiality agreements with employees, disabling access to personal data for employees who have no need to

"The upcoming NIS 2 Directive will widen the scope of the current NIS Directive, covering medium-sized and large entities from more sectors than are covered by the current Directive."

use the data and adequate contracts with data processors. It should be kept in mind that the data controller remains responsible for the data processing of its processors. Access to data should be logged and the resulting logs reviewed regularly. Adequate measures should also include clear documentation and instructions on what actions to take if an incident occurs. Timing is important; as the Dutch DPA's fine of Booking.com in 2021 shows, professional parties are expected to meet the timelines set out in the GDPR. If the cause and consequences of an incident are not yet clear, companies are advised to file a preliminary notification with the Dutch DPA, and to err on the side of caution.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

As with any other modern networked society, the Netherlands is very much dependent on digital infrastructure. Statistics by the NCSC show that the vast majority of cyberattacks concern phishing, ransomware and denial-of-service (DDoS) attacks, all of which require vastly different remedies. As a direct consequence of this diversity, the NCSC advises a varied approach. However, as a general observation it can be noted that research shows that it is essential to increase individuals' security awareness, which will not only benefit their security practices at home but also the security of the companies they work for. Updated software and regular backups (patch management) and the need for strong passwords are also essential to resilience against cyberattacks. Using professionally secured cloud services is among the general advice given to companies to increase their security. Large companies are, of course, better equipped to meet the cybersecurity challenges and may also rely on external experts to become more resilient against cyberattacks. The NCSC advises companies to divide user-accounts into low-, medium- and high-impact accounts, depending on the sensitivity of the data that the account contains and the resources that the account has access to. The report advises to implement more stricter security measures for medium- and high-impact accounts. With regard to ransomware attacks, the NCSC's recently published Incident response plan Ransomware guideline suggests how organisations can contain a breach, fix a vulnerability, remove the malware and prevent unauthorised access in the future by following the incident response cycle (Preparation-Identification-Containment-Eradication-Recovery-Lessons learned). Moreover, the NCSC recommends that organisations scale up network capacity to serve the larger number of homeworkers, to force the use of a secure connection to the corporate network through, for example, a virtual private network (VPN), to make maximum use of multi-factor authentication (MFA) for access to the corporate network and enforce strong passwords. The Dutch

DPA has also provided useful guidance to workers on how to work securely from home. It has advised them to only work from a secure work environment, to protect sensitive documents, to use (video)chat services cautiously and to be on the alert for phishing mails.

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

The controller is, and will, remain responsible and liable for any personal data he or she collects or processes. An important aspect of cloud services is the location where personal data is actually stored and processed. Under the GDPR, personal data may only be processed outside the European Union (or more precisely: the European Economic Area, EEA) if the third-country where the data is processed provides an adequate level of protection. Compliance can be achieved in various ways, all having to do with ensuring that adequate safeguards are in place within either the company or the country to which the data is transferred.

Photo: shutterstock.com/Z Jacobs

However, the EU Court of Justice's ruling invalidating the European Commission's EU-US Privacy Shield approval in the case of *Schrems II* has shown that safeguards in the context of international data transfers can be fragile. *Schrems II* has far-reaching consequences beyond Privacy Shield alone, as it has also required data exporters to conduct a so-called transfer impact assessment (or TIA) for data transfers based on Standard Contractual Clauses, and to assess whether 'additional measures' are necessary to guarantee an adequate level of protection. This judgment has put the legitimacy of international data transfers to the US (but also to other destinations outside the EEA) at risk, and the Recommendations of the EDPB that followed it, unfortunately do not offer easy solutions for all transfer scenarios either.

Currently, the main way to transfer personal data to the US on a regular basis is by concluding Standard Contractual Clauses (SCCs) combined with implementing (individual) transfer impact assessments. The newly adopted Standard Contractual Clauses by the European Commission – which will need to be implemented by 27 December 2022 – go some way to address the concerns raised by *Schrems II* and contain updated clauses that are aligned with the GDPR. Yet these SCCs can only be relied on by organisations that transfer personal data to non-EEA parties that are not subject to the GDPR. As the larger US based cloud providers will likely fall under the territorial scope of the GDPR, organisations will, strictly speaking, not be able to rely on the updated SCCs as a transfer mechanism to these cloud providers. The European Commission has recently clarified that it is in the process of creating new SCCs for transfers to non-EEA parties that are subject to the GDPR.

Possibly, this uncertain situation will be redressed by the adoption of the new 'Trans-Atlantic Data Privacy Framework'. In March 2022, the European Commission and the United States agreed in principle on a new 'Trans-Atlantic Data Privacy Framework'. The United States will have to include its commitments in an Executive Order, which will form the basis of a draft adequacy decision by the European Commission. Transfers to the UK remain lawful without the need to implement any transfer mechanism, due to the adequacy decision the Commission adopted on 28 June 2021.

These developments raise the question of whether data localisation is in fact the only robust and long-term solution likely to withstand future legal challenges. With respect to cloud services in general, the Dutch DPA has published a number of guidelines, which are in line with the Article 29 Working Party's guidance on the issue and which do not raise fundamental obstacles to the nature of cloud computing. For example, the Dutch DPA has taken the view that, even for medical data, there is no need to ask consumers for specific permission for the use of cloud hosted services. But there are also looming signs of a more restrictive view. In January 2022, the DPA published a disclaimer on its manual for privacy-friendly settings of Google

Analytics, stating that it is considering a complaint on this cloud-based website analytics tool, which may lead it to conclude that Google Analytics may no longer be used lawfully in the Netherlands.

While this indicates a general openness to cloud solutions, using cloud storage will need to be part of the overall risk assessment the controller makes before moving to the cloud, and one that may need to involve a data protection impact assessment under the GDPR. The Dutch government has itself commissioned various DPIAs into governmental use of commercial cloud services. Interestingly, these DPIAs focus heavily on the processing of diagnostic data by service providers (ie, data about the use of their cloud services, rather than the data provided by customers). The final reports, which are all available online in English, have guided the government's negotiations with a number of large international cloud providers, and have, for example, prompted Microsoft to amend its privacy policy worldwide. Last year, two cooperatives that assist Dutch schools and higher education institutions with IT procurement successfully negotiated with Google about privacy improvements for its Google Workspace for Education services.

Risk assessment does not stop once the choice has been made for a particular cloud solution: if the cloud host faces security issues, the controller will need to rethink using this particular company. A first indication of the quality of the host may be found in the availability of certificates (ISO, ISAE, NEN) concerning security. According to article 28 GPDR, adherence to an approved code of conduct may also be used to demonstrate sufficient guarantees. In 2020, the Dutch DPA approved the code of conduct submitted by NL Digital, an association of IT companies, including cloud providers. Similar codes of conduct have been approved at the EU level, most notably the CISPE Code of Conduct, which is the first pan-European sector-specific code for cloud infrastructure service providers. In February 2022, companies including Amazon Web Services, Outscale and Aruba were the first to declare that their services were in compliance with the CISPE Code of Conduct.

In order to assist controllers and processors to determine what 'appropriate technical and organisational measures' (article 34 GDPR) are, the European Union Agency for Network and Information Security (ENISA) has published guidelines that should help to answer this question by giving examples of measures. ENISA has emphasised that the guidelines do not have a 'legal status', but mainly serve as guidance for market parties. The NCSC shared its own experiences moving to the cloud which is intended to help other organisations. In addition, the NCSC published a factsheet containing five general tips in order to procure secure cloud hosting services.

Furthermore, it is advisable to address any specific concerns a controller may have in the processor agreement. In any case, the controller should ensure access to

"Risk assessment does not stop once the choice has been made for a particular cloud solution: if the cloud host faces security issues, the controller will need to rethink using this particular company. A first indication of the quality of the host may be found in the availability of certificates concerning security."

the data at all times, even in a situation of conflict with the processor. The processor agreement should also address the issue of data location explicitly, as this is a specific requirement under the GDPR and one that may be particularly challenging to address in a cloud-based setting. Other topics that warrant careful deliberation are the provider's duty to support the notification duty of the data controller if a breach should occur in the cloud provider's domain, the provider's transparency on issues like law enforcement cooperation and also the provider's role in processing metadata about the use of its services.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The NCSC was established in 2012. This public-private body advises companies and the government on the usage of software and measures to increase cybersecurity. Its aim is to make the Netherlands more resilient against cybercrime.

In its Cybersecurity Assessment Netherlands (CSAN) 2021, the NSCS concluded that digital risks to Dutch national security remain high. The coronavirus has

Photo: shutterstock.com/IvoAntoniedeRooij

accelerated the digitisation of processes and this has created more opportunities for state actors and cybercriminals to carry out digital attacks. The NSCS warns that cybercriminals can disrupt critical processes in electricity, water, healthcare and transport sectors. While the Netherlands has taken steps towards more resilience against cybercrime in the past year, the 2021 CSAN reiterates that this resilience is still insufficient and that sometimes even basic measures such as safe passwords policies are not properly implemented by organisations. In this regard, the NCSC notes that there are major differences between various companies and organisations when it comes to their resilience. It expects this disparity to grow in the future. While larger corporations have the means to spend more time and effort into the adoption of cybersecurity measures, this does not equally apply to smaller companies, while they can be targeted by sophisticated actors just as much.

In order to resist cybersecurity threats, the Digital Trust Centre (DTC) was founded in December 2020 to help increase the resilience of businesses against digital threats. Also, the NCSC was made part of the LDS, a platform in which both public and private parties, the NCSC and the DTC exchange information and knowledge about cybersecurity. This cooperation supports a more intensive information exchange between the NCSC and affiliated parties. Next to the NCSC there is also the National Coordinator for Security and Counterterrorism. This agency was established in 2012. It is an agency of the Dutch government whose aim it is to protect Dutch society against disruptive security threats. The National Coordinator for Security and Counterterrorism monitors and coordinates initiatives by the public, private and public–private sectors to strengthen cybersecurity in the Netherlands. Cooperation between the General Intelligence and Security Service, the Dutch Military Intelligence and Security Service, the NCSC, the police and the public prosecutor has also been further strengthened. Additionally, the Dutch government appointed its first Secretary of State for Digitalisation in January 2022, with tasks including monitoring the Dutch government's digital strategy and safeguarding the government's digital security.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

Companies are well advised to conduct thorough due diligence on a target's IT environment and previous experience with security incidents, which should be logged internally as a requirement of law under the GDPR. The occurrence of a security incident need in itself not be worrisome. The response of the company to the incident can be much more telling about the company's readiness and level of compliance.

When it comes to privacy and personal data, we note an increased emphasis on compliance in the context of due diligence for M&A deals. This increased emphasis is evident in various different ways. First, target companies are investigated with more scrutiny for their GDPR compliance. Second, more thought is given to the GDPR aspects of the transaction itself, such as resulting data transfers or changes to intended use of data. This, no doubt, has everything to do with the risk presented by the enormous fines that can be imposed under the GDPR for non-compliance.

There is also an increased awareness among competition authorities about the importance of vast collections of data and their potential monetary value, even if this is not necessarily reflected by equally large market shares. The Dutch competition and consumer rights authority has also highlighted the collection of data by online platforms as a potential source of market power and the Ministry of Economic Affairs and Climate Policy has suggested that upcoming mergers and acquisitions should be reviewed based on deal-value instead of the historic turnover of the companies involved.

Quinten Kroes
quinten.kroes@brinkhof.com

Marije Rijsenbrij
marije.rijsenbrij@brinkhof.com

Brinkhof
Amsterdam
www.brinkhof.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

A thorough understanding of cyber threats and the capability to work with relatively new and untested legal regimes. This requires an open mind, curiosity and creativity, and sometimes a healthy dose of paranoia about the threats. It is also important for the lawyer to have a technical interest, or background, to help in bridging the cultural divide between the IT specialists and the legal and compliance teams.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

The Netherlands is a relatively tech-savvy country, with clients approaching us with innovative and challenging legal questions. Our data protection authority has also always taken a keen interest in new technical developments such as mobile apps, facial recognition software and Wi-Fi tracking in public spaces. It has taken aggressive stances on issues such as cookie consent and legitimate interests.

How is the privacy landscape changing in your jurisdiction?

The impact of the GDPR on the Dutch society is significant. Cybersecurity has become an increasing concern, and it has become a clear government priority in the recent coalition agreement. The Dutch DPA will get increased funding from the Dutch government, and the heightened public awareness that the GDPR has caused is a key driver for further change. The Netherlands is a venue of choice for several GDPR-related damage cases.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

The Dutch DPA notes an increase in the amount of hacking, malware and phishing personal data breach notifications. The NCSC continues to warn companies about the exploitation of VPN vulnerabilities by state actors and criminals. The Dutch DPA also underlines the importance of using multiple factor authentication to prevent security incidents affecting personal data, and warns of malicious techniques such as social engineering, password spraying and credential stuffing.


d 7 32.

Switzerland

Jürg Schneider is a partner at Walder Wyss and head of its Lausanne office. His practice areas include information technology, data protection and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration and global outsourcing projects. He has deep and extensive experience in the fields of data protection, information security and e-commerce, with a focus on transborder and international contexts. He frequently publishes and lectures in his areas of focus.

David Vasella is a partner and co-head of the regulated markets, competition, tech and IP team. He advises Swiss and international clients on a wide range of IT and data protection matters, including compliance implementation projects, and provides clear and actionable advice on issues such as data protection, data monetisation, analytics, secrecy obligations, cloud outsourcing arrangements and advertising law. He frequently publishes and lectures in his areas of focus.

Hugh Reeves is a managing associate in the regulated markets, competition, tech and IP team. He advises clients in matters of technology transactions, commercial contracts, telecommunications, intellectual property and digitalisation. He is active in the areas of data protection as well as e-commerce and assists clients with their entry or expansion in the Swiss market.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

Cybersecurity is a hot topic in Switzerland. Although the number of cyberattacks is consistently growing each year, many commentators have highlighted the fact that companies incorporated in Switzerland as well as public bodies tend to underestimate or mismanage – either through a lack of clear information or of proper legal incentives – the risks posed by cybersecurity. As a result, these organisations are not sufficiently prepared to combat and withstand cyberthreats.

In light of the above, the Swiss government has been putting some effort in recent years in raising awareness among the industry and helping organisations in moving towards better cybersecurity preparedness.

At first, the Federal Council (the federal executive body) adopted a national strategy for the protection of Switzerland against cyber risks (NCS). This strategy was set up to implement a variety of measures in order to improve cybersecurity awareness and preparedness, one of them being the creation of a centralised cybersecurity body at the federal level, the National Cyber Security Centre (NCSC). This new organisation aims to create a nationwide response to cyberthreats and serves as a unified contact point for the industry.

On another level, the Swiss parliament adopted a new Federal Act on Data Protection (FADP) on 25 September 2020. This new law will enter into force on 1 September 2023. In many areas, the revised FADP has been aligned with the provisions of the General Data Protection Regulation (GDPR) applicable in the EU. However, the Swiss law does often not go into the same level as detail as its EU counterpart. Nevertheless, the revised FADP does contain its own material specificities, not the least of which is the existence of sanctions for individuals (ie, not the legal entity itself) in the event of violations of the data protection provisions. It should, however, be borne in mind that many companies active in Switzerland also fall under the scope of the GDPR, because of the orientation of their activity towards the European Economic Area (EEA).

In addition, the Federal Council suggested, in December 2020, to introduce a breach notification obligation in cases of cybersecurity incidents affecting critical infrastructure on the grounds that perpetrators of cyberattacks often use similar methods and patterns for critical infrastructure in different sectors. This breach notification obligation could thus significantly enhance the cyber resilience of critical infrastructure by quickly identifying attack methods and transmitting corresponding alerts. To date, the project has not yet materialised. However, in January 2022, the Federal Council published an explanatory report and initiated the legislative process (consultation). The consultation process ended in mid-April 2022


Jürg Schneider


David Vasella


Hugh Reeves

"There is currently no provision implementing a duty to report data breaches to an administrative body."

and should result in the adoption of a cyberattack information duty upon operators of critical infrastructure.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

Under general Swiss data protection law, there is currently no provision implementing a duty to report data breaches to an administrative body or to the data subjects themselves.

However, some commentators argue that controllers are under an obligation to do so pursuant to the principles of good faith and transparency. In addition, many controllers are bound by contractual provisions that may call for the controller's disclosure of (certain) data breaches. Furthermore, some would argue that there is a public reporting duty, based on the principles of good faith and transparency, if an individual notification to each data subject appears unfeasible or unreasonable.

This situation will change as of 1 September 2023. According to the new FADP, the controller of the data will be required to inform the Federal Data Protection and Information Commissioner (FDPIC) – the Swiss data protection authority – of any data security breach that could potentially result in a high risk to the personality rights of the data subjects. To this extent, Swiss law is expected to be somewhat more lenient than EU law, as the threshold for informing the FDPIC will be higher ('high risk' v. 'risk').

The notification will have to indicate at least the nature of the data security breach, its consequences and the measures taken or planned. The notification will have to be made as soon as possible, depending on the circumstances of the case. As a general principle, we believe that the notification period should depend on the damaging consequences of the leak. The greater the potential harm, the sooner the notification of the beach.

Furthermore, the controller must also inform the data subjects, when necessary for their protection or if specifically required by the FDPIC. This information can be restricted, postponed or waived under certain circumstances, for example, if there is a legal duty to maintain a secret, if the information is impossible to provide or requires disproportionate efforts or if the information of the data subject can be guaranteed in an equivalent manner by public disclosure.

It is important to note that the data processor will also have an obligation to notify the controller of any data security breach as soon as possible under the new law.

Under the new law, individuals who intentionally breach certain provisions of the FADP will face a criminal fine of up to 250,000 Swiss francs. This is significantly

"Under the new law, individuals who intentionally breach certain provisions will face a criminal fine of up to 250,000 Swiss francs. This is significantly higher than under applicable law, where breaches can be sanctioned with a maximum fine of 10,000 Swiss francs."

higher than under applicable law, where breaches of the FADP can be sanctioned with a maximum fine of 10,000 Swiss francs – and only under certain restrictive circumstances. However, failure to report a data breach incident does not directly fall under the scope of these criminal sanctions. Accordingly, there will be no criminal prosecution for a reporting duty breach under the revised FADP, though a sanction can be levied if it appears that the minimum data security requirements were not in place.

Furthermore, the FADP states that if an organisation notifies a data breach in accordance with its obligation pursuant to the new law, this notification may not be used in criminal proceedings against the person obliged to notify without its consent. The protection of the data controller is thus reinforced. This provision intends to encourage organisations to report any data security breach in compliance with the law, without having to fear for a conviction in a subsequent criminal proceeding.

Despite the absence of any criminal sanctions, an organisation failing to report a data security breach may expose itself to a serious reputational harm if the information goes public through other channels. Therefore, organisations would generally be well advised to strictly adhere to the legal framework, which they should interpret in a prudent (ie, expansive) manner.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

The main issues can be subdivided into four chronological phases that a company has to go through when suffering a data security incident.

First, organisations must determine the exact cause of the cybersecurity incident. It is very important to know whether the incident is due to a technical issue or if the company was subject to a cyberattack. This will then allow the organisation to take adequate measures to remedy the data security incident (internally or with involved third parties such as storage providers). Once the cause of the incident has been identified, the organisation should also be able to assess whether the incident is over or whether it is still ongoing, as may be the case if an ill-intentioned actor revealed a backdoor in the company's IT systems and shared those revelations with third parties.

Second, but in parallel, organisations must determine the exact impact of the cybersecurity incident. Importantly, organisations must know as quickly as possible whether data was potentially stolen, disclosed or lost. If so, the exact scope of the data incident must be clarified, particularly if personal data or confidential information affecting contractual partners are impacted.

Photo: shutterstock.com/MaykovaGalina

Third, under the revised FADP, if it appears that personal data or confidential information was impacted by the incident, the company's management or another designated person within the company must determine whether there is a high risk that the personality rights of the data subjects may be violated. More often than not, this will be the case at this stage, as it is rather difficult to categorically exclude the infringement of personality rights of data subjects. It should also be borne in mind that organisations are required to make a quick decision in this situation, which should lead them to admit the existence of such a risk, except in few rare cases.

Fourth, still under the new law, if there is a high risk for the personality rights of the data subjects, the company's management or another designated person within the company must decide whether or not the company should notify the data breach to the FDPIC or the data subjects themselves. Regarding the factors and risks to be considered in this respect, reference is made to the developments in question 2.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

An initial step is to assess the level of compliance with the GDPR. Many Swiss-based companies already fall under the scope of the GDPR, given the latter's extraterritorial scope of applicability. These businesses therefore need to aim for GDPR compliance. As a result, companies in Switzerland had to bolster their data security and adopt mechanisms to prevent data breaches in accordance with the requirements under the GDPR. That said, those organisations that already comply with EU law will largely be prepared under the revised FADP as well.

Nevertheless, some adjustments may be necessary to meet the specific requirements of the revised FADP. For instance, businesses would be well-advised to perform an audit of the existing internal data protection processes or perform a specific risk assessment. This could give rise to a need to review and enhance processes, practices, documentation, contracts, policies and notices, and a need to establish new ones.

Companies should however not only focus on adopting measures to prevent the risk of cyberattacks, but also on developing internal regulations as to how to react to a data breach. Proper management of a cybersecurity crisis is more effective if organisations have clear guidelines in terms of competences and procedures. The individuals in charge must me able to follow a straightforward procedure to determine the cause of the data breach as quickly as possible and to determine whether data has been impacted or not. This gives companies a vital safety belt in a time where fast thinking and swift decisions are key.

In any event, organisations must assess on a case-by-case basis the extent to which their data protection processes need to be adjusted. Swiss companies that do not fall under the scope of the GDPR and have not implemented any changes thereunder will likely need to put in additional effort towards compliance with the revised FADP.

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

The use of cloud services is widely accepted in Switzerland and is often a better choice in terms of data security in comparison with an internal IT storage set-up. This is because third-party cloud providers need to be constantly up to date with the latest technological evolutions to achieve adequate data security. To that extent, they can be seen as specialists in their field of expertise. In addition, cloud providers often have deep and extensive experience in the hosting area. Therefore,

> "The use of cloud services is widely accepted in Switzerland and is often a better choice in terms of data security in comparison with an internal IT storage set-up."

transferring data to a reputable cloud hosting environment is often seen as a best practice in terms of data security.

One talked about topic is the relevance of certifications when it comes to choosing between different cloud hosting services. Swiss law imposes a general obligation on cloud providers to ensure adequate data security. For that purpose, many cloud service providers have sought to obtain data security and cybersecurity certifications, aiming to reassure potential clients that their data is in good hands. That said, certifications should still be seen mostly as a form of guidance rather than any exhaustive guarantee as to service quality. In any event, clients should also choose a cloud provider considering other factors, such as business continuity, key performance indicators and adequate support level.

On the other hand, privacy becomes a serious issue when transferring data to a cloud hosting environment, especially if the provider is located abroad in a country that is not deemed to have an adequate level of data protection in its own legal landscape. The country in which the hosting (or data access) occurs will inform any additional steps, such as conducting a data transfer impact assessment and

safeguards, the parties will need to take. Failure to take these measures could qualify as a breach of the Swiss data protection legislation.

As a result, in a cloud services scenario, the parties may have to conduct a data protection impact assessment and implement additional safeguards in cases of cross-border disclosure or storage of personal data. One way to compensate for the lower level of data protection is to incorporate contractual clauses, especially the 'Standard Contractual Clauses of the European Commission', adapted to Switzerland.

In summary, the reliance on an external cloud hosting environment is, for the data controller, very much a balancing act between the numerous technical advantages, on the one hand, and the need for a correct legal assessment and set-up on the other.

Photo: shutterstock.com/RudyBalasko

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

As mentioned in question 1, the Swiss government adopted the NCS and set up the NCSC. This has primarily helped to achieve awareness among the various actors of the market regarding the risks posed by cyberattacks.

On 18 May 2022, the Federal Council took note of the report on the effectiveness assessment of the NCS and decided to create a further 25 positions in the area of protection against cyber risks. It also decided to turn the NCSC into a federal office and instructed the Federal Department of Finance (FDF) to prepare proposals by the end of 2022 regarding how the office should be structured and which department it should be part of. This demonstrates a firm intention to further strengthen the nationwide response to cybersecurity threats and criminal activity.

Moreover, the Swiss Federal Council initiated steps towards adopting policies and regulations concerning the specific topic of cybersecurity. This represents a break from the past, as cybersecurity was traditionally addressed as a subtopic of data protection and data security. The recent developments have shown that cybersecurity is now a focus for the Swiss government.

Despite the above, the Swiss legislative process is comparatively slow. For this reason, the current discussions surrounding cybersecurity are not expected to lead, in the short term, to the adoption of an overarching legislative act on cybersecurity standards.

Nonetheless, the absence of clear cybersecurity standards on the legislative level has paved the way for some public-private organisations to contribute to the development of a response against cyberthreats in Switzerland. For example, a private–public initiative was created under the name 'Trust Valley'. This project aims to further enhance Switzerland's position as a hub for matters of digital trust and cybersecurity. On another level, the DiploFoundation, the Federal Department of Foreign Affairs (FDFA) and the Federal Office of Communications joined forces to create the Geneva Internet Platform, a discussion centre for digital policy matters, including those pertaining to cybersecurity.

In addition, cybersecurity has also become a favoured topic for higher education institutions, which often have specialised centres focusing on this manner. This is, for instance, the case for the Swiss Federal Institute of Technology in Zurich (ETH), which opened a Center for Security Studies. A similar study path was launched at the Swiss Federal Institute of Technology in Lausanne (EPFL), resulting in the setting-up of the Center for Digital Trust (also known under the moniker C4DT).

Furthermore, the ETH and the EPFL have joined forces with the national defence in creating the 'Cyber-Defense Campus' under federal direction, which brings

together governmental, academic, and industrial actors to reflect on cybersecurity in the context of national defence.

The above-mentioned initiatives show that Switzerland is committed to promoting a solid response towards cyberthreats.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

M&A deals are truly multifaceted as they involve many legal considerations. We can highlight the following.

From the selling company's perspective (ie, the company that should be acquired at the end of the deal) it must be kept in mind that, in the near or medium future, its data will often be stored with the acquiring company's data (meaning on common servers or with a common provider). The buyer will rarely be interested in relying on separate IT systems or on separate hosting providers, because doing so would not only increase costs, but would complicate the management of the IT systems and data storage. Even in the case of fully separated data storage, the acquiring company will usually and eventually have the right to access all the selling company's data, by simple virtue of being the owner or majority shareholder of the selling company. This is true in particular in the case of 'share deals'. In the case of 'asset deals' where there is no change of hands of the shares and the rights attached thereto, the situation can be comparable – or even more drastic – as the transferred assets may include data sets. The selling company will also need to ensure that it may disclose certain information, such as employee names, during the due diligence process leading up to the M&A deal, as failing to do so could give rise to liability in particular under data protection law.

Though the concerns raised above are often harmless in practice, such deals could have a negative impact, at least to the reputation, for a selling company that built its reputation, for instance, on outstanding data security or on storage solely in a given jurisdiction (as is frequently the case). The selling company should therefore carefully consider this point and determine if it wishes to risk its hard-earned market reputation.

From the buyer's perspective, data security issues are a hot topic. A data breach could involve the loss of valuable trade secrets, such as secret recipes, client lists, production methods and so forth. Moreover, the reputational harm frequently associated with (publicised) data breaches not only risks spreading to the buyer but also may reduce the market value of the selling company's trademarks as well as its market valuation. As an example, publicly traded companies tend to experience a noticeable dip on the stock market if they suffer a cybersecurity event. Also, under

"From the buyer's perspective, data security issues are a hot topic. A data breach could involve the loss of valuable trade secrets, such as secret recipes, client lists, production methods and so forth. Moreover, the reputational harm frequently associated with (publicised) data breaches not only risks spreading to the buyer but also may reduce the market value of the selling company's trademarks as well as its market valuation."

the GDPR, data breaches may lead to high fines. As these fines are calculated on the entire group turnover, acquiring a company that is still breaching data protection rules could have an even higher financial impact. For this reason, conducting an extensive privacy and data security due diligence is of essence in any M&A deal.

Of course, data protection in general is an important topic as well, because the buyer will want to ensure that it can use the data for its business after the deal. This would be difficult or even impossible if the data was not lawfully collected, for instance.

Jürg Schneider
juerg.schneider@walderwyss.com

David Vasella
david.vasella@walderwyss.com

Hugh Reeves
hugh.reeves@walderwyss.com

Walder Wyss Ltd
Lausanne and Zurich
www.walderwyss.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Cybersecurity is very much an area where experience is necessary. That said, clients should ultimately base their choice on personal preference. When dealing with cybersecurity, a lot of the underlying information is highly sensitive, and the client–attorney relationship will need to rely on the highest level of trust in order for it to bear fruit.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

First, the relevant technologies are evolving very rapidly. We enjoy following technological evolutions and catching a glimpse of tomorrow's technologies. Second, we are frequently dealing with international matters. This multinational context is rife with complexities but is, for that very reason, a real pleasure to work with.

How is the privacy landscape changing in your jurisdiction?

A fully revised data protection act was adopted by Parliament in September 2020, and this piece of legislation is expected to come into force on 1 September 2023. This new law is going to bring closer alignment to the EU's GDPR. We are also following with a lot of interest the public dialogue around privacy. These are reflected in the discussions surrounding telecommunications surveillance, which often boils down to strong privacy prerogatives versus governmental access to personal information for security purposes.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

Ransomware and attacks aiming at the theft of trade secrets are two types of incidents that require constant and high awareness. That said, companies need to evaluate their cybersecurity worst case scenario individually. Even though companies can evaluate cyber risks on a general level, they are also right to keep in mind that their situation is always unique and requires a tailored approach.

Taiwan

Ken-Ying Tseng currently heads Lee and Li's digital, TMT and data privacy practice group. Before 2018, she was the head of Lee and Li's M&A practice group for 12 years. She received an LLM from Harvard Law School. Ken-Ying advises on various forms of mergers and acquisitions, and is experienced in resolving both legal and commercial issues. She assisted and represented several multinational corporations in their M&A activities, including Affinity, TPG, Aleees, McDonald's, Sony, Energy Absolute and Qualcomm.

In addition to M&A, Ken-Ying constantly advises various tech companies that are in the businesses of social networks, instant messengers, search engines, portal sites, sharing economy, e-commerce, OTT, online games, P2P lending, e-payments and cloud computing. Ken-Ying also frequently advises clients, including multinational companies, on privacy and data protection (GDPR), e-marketing, big data, e-signature, domain name, telecommunications, satellite, fintech, artificial intelligence, cybersecurity, internet governance and other legal issues.

Ken-Ying is admitted to practise law in both Taiwan and New York.

She has been honoured in Taiwan's Top 100 Lawyer, 2022, *Asia Business Law Journal*, *Asialaw Distinguished Practitioner 2022* in Corporate and M&A, *IFLR 1000*, Leading Lawyer, Highly Regarded, 31st Edition and Most Influential Woman in Personal Data Protection Law 2019 – Taiwan, Acquisition INTL.

Ken-Ying holds other positions, namely the managing director, Taiwan Internet Government Forum (TWIGF), member of the International Affairs Committee of TWNIC Supervisor, Taiwan Internet and E-commerce Association, supervisor of the National Information Infrastructure Enterprise Promotion Association and director of Secure On-line Shopping Association of Taipei City.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

The Cybersecurity Management Act (the Cybersecurity Act), the Enforcement Rules of the Cybersecurity Act (the Enforcement Rules), as well as may other regulations promulgated under the Cybersecurity Act, became effective on 1 January 2019. Pursuant to the Cybersecurity Act and the relevant regulations, such as the Regulations for Classification of Cybersecurity Responsibility, cybersecurity responsibility is further classified into five levels (from Level A to Level E). Each government agency must stipulate its own cybersecurity maintenance plan and also set forth the guidelines on the cybersecurity matters for the 'specific non-governmental agencies' that it regulates. Many government agencies have promulgated such guidelines to regulate the 'specific non-governmental agencies' subject to their jurisdiction.

At the end of March 2021, the Executive Yuan passed a series of bills to establish a new ministry, the Digital Development Ministry, which will be in charge of cybersecurity matters as well as other digital development-related matters in the future. The new ministry was expected to be established in June 2022 and will commence operation soon.

Meanwhile, with regard to the financial industry, in August 2020, the regulator of the financial industry, the Financial Supervisory Commission (the FSC), announced its new agenda to improve cybersecurity of the financial industry. Pursuant to the new agenda, the FSC plans to amend the existing internal rules and self-regulations of the various financial institutions so as to include new cybersecurity standards into the existing rules. Following the FSC's above initiatives, in April 2021, the Taiwan Stock Exchange announced a new requirement under which listed companies are mandatorily required to make public announcement or hold press conference in the event of a material cybersecurity incident that may cause material harm to the listed company or impair the operation of the listed company. In December 2021, the FSC further amended the Regulations Governing Establishment of Internal Control Systems by Public Companies requiring a listed company with paid-in capital of NT$10 billion or more or with a market value among one of the top 50 in the Taiwan stock market to hire a chief information security officer.


Ken-Ying Tseng

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

Pursuant to the Cybersecurity Act, the agencies subject to the Cybersecurity Act shall report to its supervisory agency, or to the competent authority of the industry that the private agency is engaging in, as applicable when the agency becomes aware of a cybersecurity incident. A cybersecurity incident refers to any incident under which the system or information may have been accessed without authorisation, used, controlled, disclosed, damaged, altered, deleted or otherwise infringed, affecting the function of the information communication system, and thereby threatening the cybersecurity policy. Hence, as long as there is a security breach incident, even if no 'personal data' is involved, the incident may be subject to reporting requirements.

The Regulations for Reporting and Responding Cybersecurity Incidents set forth further details about the reporting of cybersecurity incident as required under the Cybersecurity Act. A 'specific non-government agency' shall report to its regulator at the central government within 'one hour' after it becomes aware of the

"A cybersecurity incident refers to any incident under which the system or information may have been accessed without authorisation, used, controlled, disclosed, damaged, altered, deleted or otherwise infringed, thereby threatening the cybersecurity policy."

cybersecurity incident, and the regulator shall respond within two to eight hours depending on the classification of the cybersecurity incident. In the meantime, the specific non-government agency shall complete damages control or recovery of the system within 36 to 72 hours depending on the classification of the cybersecurity incident.

Meanwhile, if personal data is involved in a data breach incident, pursuant to the Personal Data Protection Act (the PDPA), either a public agency or a non-public agency shall inform the affected data subjects of the data breach incident as soon as it inspects the relevant incident. In the notice to the data subjects, the relevant facts concerning the incidents, such as what data was stolen, when the incident happened, the potential suspect that breached the data and the remedial actions that have been taken shall be described. The PDPA does not set forth any threshold of the notification to the affected data subjects.

On the notification to the regulator, the PDPA does not specify any obligations to report a data breach incident to the regulator. However, in the personal data security maintenance plans stipulated by the competent authorities of each industry, the regulator may require the private sector to report a data breach incident to it within a 72-hour period. As of the end of 2021, the competent authorities of many industries have included the data breach incident reporting requirement in the personal data security maintenance plans that they stipulated. As a result, many industries in Taiwan are now subject to a 72-hour reporting requirement under which they shall report to their competent authority a data breach incident within 72 hours of becoming aware of the occurrence a data breach incident. In most of the cases, the reporting will only become mandatory when the data breach incident is deemed 'material'. Some of the competent authority has adopted its own definition of 'material', such as 'affecting the daily operation' of the private business.

Furthermore, financial institutions shall asses if the incident materially impacts their operations. If so, they will need to report to their respective primary regulators and take responsive actions as required by the relevant regulations.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

The most important issue for a company facing a data security incident shall be how to prevent further damage or harm that may be caused by such an incident. If possible, a company shall notify the affected data subjects as soon as possible so that they are alerted and have the chance to take precautionary measures (for example, resetting their passwords) in time. A company shall also take immediate

actions to detect and fix the loophole in its system, if any, to prevent any further breach or damages.

In many of the data security incidents that are locally reported, the cause of the incident is not system failure or hackers' activity but the misconduct of the relevant employees, contractors or the employees of the contractors. Hence, it is very important for a company to adopt proper security measures and internal control rules, awareness training and standards for employees/contractor selection. Often, the data breach incident could be caused by the mistake made by the staff of small service vendors, but the large companies retaining their services would be forced to deal with the customers who may suffer damages. At the end, cases would be settled because the small service vendors may not be financially capable of bearing the relevant liabilities but the large companies need to protect their brand names. Hence, a company needs to carefully select its service vendor, and in the service agreements, clauses addressing to personal data protection and indemnification liabilities shall be included.

Photo: shutterstock.com/NH

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

In Taiwan, most of the businesses are cost-sensitive small or medium-sized enterprises, and they tend to believe that adopting a certain 'one-stop' solution (ie, installing a certain 'package software') can handle the cybersecurity issues as well as compliance of the applicable privacy laws, including GDPR. This is, of course, not the case. Even purely from an IT perspective, installing package software may not be sufficient in protecting the businesses from cyberattacks.

Large corporations are more cautious and normally will hire IT specialists or consultants/lawyers to implement security measures, to conduct internal training and to design standard operating procedures (SOPs), etc. They will also seek internationally recognised certifications, such as ISO27001. Some of the industries are required to pass ISO27001 certifications, such as the telecommunications industry.

Companies may also consider joining certain alliances, such as TWCERT, to obtain or share intelligence in relation to recent cybersecurity threats and relevant resources.

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

Pursuant to the PDPA, a cloud service provider will most likely be deemed as a data processor while the business using the cloud service will be deemed as the data controller. Pursuant to the PDPA, the data controller shall be held liable to its customers if the cloud service provider/data processor does not comply with the PDPA or the instruction of the data controller. The data controller may also have administrative fines imposed for any breach of the PDPA by the data processor. Hence, it is important to select a trustworthy cloud service provider when a business decides to move its data to the cloud.

The business shall also check whether it is subject to any special sector regulations for outsourcing data processing or storage or even storing data outside of Taiwan. For example, financial institutions are subject to the prior approval of the competent authorities for outsourcing activities even locally. The regulatory approval in this regard is rather burdensome. Furthermore, for some industries, customers' data are prohibited from being stored in China, such as telecommunications operators and TV channels, cable TV system operators and social worker firms.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The websites and systems of the Taiwan government, as well as large corporations, have been frequently hacked or attacked by attackers outside of Taiwan, such as from China. The cyber army of China was blamed for most of the attacks and incidents. Meanwhile, recent incidents involving 'fake news' or misinformation that have been alleged to be posted by Chinese on Taiwanese websites also triggered the attention of the Taiwan government. To protect the cybersecurity of Taiwan, the Executive Yuan initiated a series of actions, including the implementation of the Cybersecurity Act. By imposing the relevant requirements under the Cybersecurity Act, such as strengthening the regulated agencies' internal procedures and SOPs, the government was hoping to raise the cybersecurity standards in Taiwan as well as the ability to fight against cyberattack. The government also hopes to foster the growth of the local cybersecurity industry through the implementation of the Cybersecurity Act as there will be more audit tasks to be conducted by the regulated agencies.

Given that now cybersecurity is national security, the National Security Act was amended in 2019, which claims and explicitly states that the protection of national security shall include the protection of the security of cyberspace, as well as physical space, in the territory of Taiwan. This means that the application of the National Security Act to the activities conducted on the internet is now officially confirmed, without the need for further interpretation.

With regard to the prevention of criminal activities, the Taiwan government has long established a special task force, the 9th Investigation Corp of the Criminal Investigation Bureau (CIB), to combat criminal activities conducted via high-tech or information technology, such as computer crime, cybercrime, and so on. All of the cyber-related crime activities reports will be forwarded to the 9th Investigation Corp for further investigation. The 9th Investigation Corp is equipped with police officers with technology backgrounds as well as high-tech hardware and software. It has established channels with police authorities in other countries to investigate cross-border crimes. To combat 'phone fraud' activities, the National Police Agency further established a special phone line, '165', to assist the general public in fighting against the fraudsters.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

An acquirer or surviving entity in an M&A deal needs to evaluate the potential risks from the following perspectives.

"In many of the data security incidents that are locally reported, the cause of the incident is not system failure or hackers' activity but the misconduct of the relevant employees, contractors or the employees of the contractors. Hence, it is very important for a company to adopt proper security measures and internal control rules."

The first perspective is the track record of the target. The past records of data breach incidents, and notable non-compliance of privacy laws, can be used to calculate the existing or contingent liabilities of the target, as well as the pattern for future liabilities in the event that the target continues its operation in the same manner after the M&A.

The second is data ethics. If the target constantly ignores cybersecurity threats or disrespects privacy or data ethics, there may be unpredictable contingent liabilities already.

The third is costs for future reform. In addition to the liabilities evaluation stated above, the acquirer or surviving entity shall also estimate the costs to fix the existing issues and to reform the operation. This will include the costs for: (i) IT technology, (ii) obtaining proper consents from the data subjects, and (iii) performing notification obligations to the data subjects.

The forth is the losses to be incurred due to reduction of customer database. Customer data without proper consents would need to be eliminated and the losses of business opportunities shall also be considered and calculated.

Ken-Ying Tseng
kenying@leeandli.com

Lee and Li, Attorneys At Law
Taipei
www.leeandli.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

The lawyer must have sufficient experience, knowledge and training to think and act fast. Meanwhile, a cybersecurity incident may not be handled merely from a legal perspective, and sometimes, the client would need to deal with government relationship as well as public reputation or relationship. The lawyer needs to be able to take all of the relevant factors into consideration when rendering legal advice.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

I found cybersecurity and privacy practice fascinating because I would encounter cutting-edge legal and commercial issues and need to respond simultaneously, while addressing all of the potential legal liabilities and consequences to the clients. I need to be creative in order for the client to obtain the required consents from the data subjects.

How is the privacy landscape changing in your jurisdiction?

Taiwan adopted a legal framework of personal data protection that is similar to the EU data protection laws. Some of the provisions are even stricter, and Taiwan is one of the very few countries without a centralised data protection authority. Taiwan has submitted its application for a GDPR adequacy decision in 2018 and is in the process of negotiating with EU. The Taiwan government may reform the privacy law to be more GDPR compliant and take the same position as the EU for similar issues.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

In April 2021, international news media revealed that Quanta Computer, the key supplier of Apple, was hacked by the ransomware group REvil, also known as Sodinokibi. It was reported that REvil requested a ransom of around US$50 million. Taiwan is the leading country manufacturing semiconductors, and there are also many other tech companies playing important roles in the global supplier chain, so is very important to make the extra effort to prevent cybersecurity incidents.

United States

Jason Chipman is a WilmerHale partner who advises companies on complex regulatory matters associated with data security, cyber incident response, the Committee on Foreign Investment in the United States and related export controls. He has assisted companies in most sectors of the economy on data security best practices and frequently assists with corporate due diligence. Mr Chipman currently serves as a non-resident fellow at the National Security Institute.

Benjamin Powell is a WilmerHale partner who has advised companies on major cybersecurity incidents and preparedness across virtually every sector, including banking, investment management, retail, defence and intelligence. He is recognised as a leading attorney in international investment and mergers, including the Committee on Foreign Investment and the Defense Security Service.

Arianna Evers is a WilmerHale special counsel who advises clients on complex privacy, data security and consumer protection issues arising under rapidly evolving federal and state requirements. She regularly assists clients on privacy-related issues, including legal requirements and best practices in emerging and changing areas of the law, and also represents them in regulatory investigations.

Shannon Togawa Mercer is a WilmerHale senior associate who advises clients on matters related to cybersecurity, privacy, and US and European data protection. She joined WilmerHale from the London location of a large global law firm where her practice focused on transactional work, including the cybersecurity and data protection aspects of capital markets transactions and mergers and acquisitions.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

There is a growing trend toward more proscriptive cybersecurity requirements in economic sectors perceived as playing a critical role in the US economy or for US security. For example, in March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 was signed into law, which requires critical infrastructure entities to report material cybersecurity incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA). Additionally, in April 2022, a final rule issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation took effect, which requires banking organisations and their bank service providers to report any significant cybersecurity incident within 36 hours of discovery. The Securities and Exchange Commission has also proposed rules that are intended to enhance disclosures about cybersecurity risk management, strategy, governance and incident reporting by public companies. These recent developments align with President Biden's Executive Order on Improving the Nation's Cybersecurity (the Cybersecurity EO), which sets out to improve cybersecurity, particularly in relation to federal government systems, and followed several high-profile cyber incidents in 2020 and 2021. Companies that do business with the United States government face increasingly strict data security requirements for how they manage, store and process sensitive government information, with mandatory reporting of data breaches and standards for safeguarding sensitive data. For example, the Cybersecurity EO includes updates to federal contracting language involving cybersecurity incident reporting, which may eventually be implemented through Federal Acquisition Regulatory Council rules. Under the Cybersecurity EO, the National Institute of Standards and Technology (NIST) also issued guidelines related to source code testing for software developers acting as government vendors.

At the same time, legislators at the state and federal level are exploring the creation of privacy rules that include mandatory data safeguarding requirements for personal information. There are five US states with comprehensive privacy laws – Colorado, California, Virginia, Utah and Connecticut – and many other states are exploring potential new laws as well; these laws generally require that entities provide reasonable administrative, technical and physical security practices to protect personal information. Congress held multiple hearings in 2021 and early 2022 to investigate a perceived need to pass a comprehensive federal data protection law. We anticipate these trends will ultimately (although perhaps not expeditiously) lead to more uniform and clear cybersecurity standards, along with


Jason Chipman


Benjamin Powell


Arianna Evers


Shannon Togawa Mercer

> “States are continuing to expand their definitions of covered information.”

related privacy rules. In the meantime, federal agencies in the United States are likely to continue efforts to aggressively police cybersecurity regulatory compliance applicable to particular economic sectors and to seek to impose new requirements on companies responding to breaches.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

The United States does not have a uniform data breach notification law. Rather, all 50 states, as well as the District of Columbia and a number of territories, have individual data breach notification laws. At the federal level, sector-specific laws for government contractors, certain financial institutions and certain businesses handling health records also impose special breach notification rules. In general, data breaches mandate notification to regulators and consumers when specific categories of sensitive personally identifying information are compromised through a cyber intrusion, inadvertent disclosure or other loss of data. For example, in many

jurisdictions, the unauthorised acquisition of or access to data that includes name combined with a social security number, financial account number, driver's licence number, health record or passport number would likely trigger a mandatory breach notification obligation to the consumer and may also trigger notification obligations to regulators. States are continuing to expand their definitions of covered information, with username or email address in combination with a password or security questions and answers as well as biometric data becoming subject to breach notification requirements. State regulators are also increasingly investigating cyber incidents and bringing enforcement claims for perceived lapses in reasonable cybersecurity controls.

3 | What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

Data security incidents, particularly cyber intrusions, may raise many significant challenges. For companies handling substantial amounts of sensitive personal information, such incidents may trigger:

- communications challenges for companies that want to provide consumers or other customers with reassurance while also investigating the scope of a particular incident;
- reputational and financial challenges as incidents can impact brand stability, stock price, and a company's relationship with customers and other third parties that do business with it;
- remediation challenges in taking steps to further safeguard sensitive data to both stop a cyber intrusion and to help bolster existing security; and
- investigative challenges to determine the scope of the intrusion, what data was taken and whether the attacker has been removed from the company's networks.

Managing these sorts of challenges, often while also coordinating with law enforcement authorities, regulators, stakeholders and affected individuals, requires all components of a business to work together. Such incidents are not just the province of the information technology team. They are, rather, problems that require senior attention to manage and address.

4 | What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Incident response requires an immediate, coordinated effort to gather the facts through forensic analysis and to execute an incident response plan that enables the

company to address multiple work streams simultaneously in a coordinated fashion. The response generally prioritises remediation, reputational harm, communication with all the relevant constituencies (including, critically, customers) and preparing for the range of potential regulatory inquiries and litigation.

Companies can take several steps to best prepare for and improve their ability to respond to such issues, including:

- reviewing existing incident response plans, benchmarking against industry best practices on a regular basis, and proposing changes. Plans should also be reviewed after any serious incident to incorporate lessons learned from the company's response to that incident;
- developing and participating in tabletop exercises to help those with implementation responsibilities understand how the incident response plan would work in practice;
- engaging third-party firms in advance, through counsel, to ensure that the right resources are available to address critical issues in a time-sensitive manner and under attorney–client privilege;
- conducting regular risk assessments of a company's information technology infrastructure, systems and controls to identify and mitigate risk to the extent that risk does not align with the entity's business goals;
- providing regular updates on, and analysis of, legal and regulatory developments that would influence response plans and practices; and
- training employees, not just those involved in information security, to recognise potential security risks.

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

Cloud services trigger a variety of risks that should be carefully balanced as part of the decision to outsource data storage or other information technology functionality. Although cloud computing is somewhat new for many organisations, the risks associated with cloud computing are similar to other types of IT outsourcing. Those risks include the following:

- third-party access to data. When company information is outsourced for storage or other processing by third parties, that information may no longer be solely within the control of the information owner. The cloud provider may be compelled to release it to third parties in litigation or to government agencies inside or outside the United States. Moreover, absent appropriate prohibitions in the parties' agreement, a cloud provider may be entitled to share customer data

(or data derived from customer data) with third parties for the cloud provider's own business purposes;

- data security. Evaluating the security of data in a cloud environment and ensuring the use of appropriate safeguards can be very challenging. Many cloud providers will not provide full visibility into their own network security posture;
- location of data. Data entrusted to a third party may be stored or otherwise processed in a jurisdiction that gives rise to unique legal or regulatory concerns. Moreover, some cloud providers do not provide transparency or assurances concerning where the data will be located;
- privacy and consumer notice. Processing of consumer data by a third-party cloud provider may necessitate special notices to consumers or employees and it may trigger a number of privacy and data protection obligations with respect to how their data will be handled, retained and distributed; and
- business continuity or provider lock-in. Cloud providers and sub-processors may go out of business or otherwise experience a disaster or other incident that results in the loss, corruption or temporary inaccessibility of their customers' data. Further, it may be difficult to extricate data from a software as a service

Photo: shutterstock.com/SeanPavone

"Legislators at the state and federal level are exploring the creation of privacy rules that include mandatory data safeguarding requirements for personal information."

solution at the end of the parties' engagement, at least in a format that does not require substantial processing before the data can be ingested into a competitor's software as a service product.

There are a wide range of different regulatory regimes that impact cloud outsourcing. Some regulations that are agnostic about whether data is outsourced in a cloud environment or remains within a company's firewall, impose general obligations that have the effect of imposing rules that data owners must satisfy in a cloud scenario (such as National Institute of Standards and Technology requirements to track and specially secure sensitive data). Other regulations are cloud-specific, such as ISO 27017, an independent security standard that provides guidance on the information security aspects of cloud computing and is often used by organisations to judge their ability to manage data in a cloud environment. Certain sectors, particularly the financial services and government contracting sectors, are subject to more stringent requirements on their use of cloud services to host consumer or government data.

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

Cybersecurity remains a substantial focus of federal and state law enforcement efforts in the United States and is an area of particular concern as destructive ransomware events become more common and more substantial. The Federal Bureau of Investigation has grown its cyber capabilities substantially over the past several years, and President Biden's administration is increasingly focused on efforts to combat ransomware groups.

Specific laws that address criminal activity in the cyber context include the Computer Fraud and Abuse Act, which outlaws intrusions into or interference with the security of a government computer network or other computers connected to the internet. In addition, several federal surveillance laws prohibit unauthorised eavesdropping on electronic communications, which can limit a variety of cybersecurity activities. For example, the Electronic Communications and Privacy Act prohibits unauthorised electronic eavesdropping. The Wiretap Act prevents the intentional interception, use or disclosure of wire, oral or electronic communication, unless an exception applies. The Stored Communications Act precludes intentionally accessing without authorisation a facility through which an electronic communication service is provided and thereby obtaining, altering or preventing authorised access to a wire or electronic communication while it is in electronic storage.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

Cybersecurity and privacy is increasingly a significant topic for M&A due diligence because of potential regulatory or litigation exposure that a company may take on through an acquisition. Acquirers often seek special assistance to evaluate the scope of exposure by examining the nature of the target business, the type of data it collects, maintains and shares about customers or third parties and the regulatory environment in which it operates. Acquirers may also evaluate the types of controls the company has in place to protect its systems, limit data sharing to permissible means and otherwise ensure compliance with regulatory requirements. After the transaction is complete, acquirers need to pay close attention to ensure that the target company is either fully integrated or that the target's privacy and data security practices are brought into line with the acquirer's risk tolerance.

Jason Chipman
jason.chipman@wilmerhale.com

Benjamin Powell
benjamin.powell@wilmerhale.com

Arianna Evers
arianna.evers@wilmerhale.com

Shannon Togawa Mercer
shannon.mercer@wilmerhale.com

Wilmerhale
Washington, DC
www.wilmerhale.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Legal advice around cybersecurity issues requires counsel that is experienced at addressing and managing the wide range of issues that cybersecurity incidents and related preparation activities may trigger.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

Cybersecurity is an evolving and changing field that requires lawyers to provide a mix of legal, policy and business guidance to clients navigating new and often challenging issues. An increasingly large number of federal and state regulatory agencies, categories of litigation plaintiffs and business partners are interested in understanding how companies are protecting their data, resulting in an increasingly complex web of risks.

How is the privacy landscape changing in your jurisdiction?

Privacy is becoming a critical part of contracting arrangements between parties, with greater focus on compliance with state, national and international laws. Greater regulation of the handling, securing and transfer of data is resulting in an increasing focus by companies on privacy issues, particularly on specifying the obligations that must be met in the handling of data between parties. The California Consumer Privacy Act of 2018 went into effect in 2020, and new laws in California, Utah, Connecticut, Virginia and Colorado will go in to effect in the near term.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

Understanding about cyberthreats is generally increasing in the United States. High-profile incidents involving espionage and criminal actors receive frequent public attention. But companies need to be constantly on guard for the latest threats. In the recent past, incidents involving tax fraud were on the rise and today ransom and extortion demands associated with cyber intrusions are becoming more common.

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by WilmerHale, this Privacy & Cybersecurity volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals.

Regulatory trends
Cloud hosting
M&A risks
Selecting counsel

ISBN 978-1-83862-999-1