GIR INSIGHT

ASIA-PACIFIC INVESTIGATIONS REVIEW 2020

ASIA-PACIFIC
INVESTIGATIONS REVIEW 2020

Reproduced with permission from Law Business Research Ltd
This article was first published in September 2019
For further information please contact Natalie.Clarke@lbresearch.com

LAW BUSINESS RESEARCH

Published in the United Kingdom
by Global Investigations Review
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street, London, EC4A 4HL

www.globalinvestigationsreview.com

To subscribe please contact subscriptions@globalinvestigationsreview.com

ISBN: 978-1-83862-225-1

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Cross-border overviews

Country chapters

Preface

Welcome to the *Asia-Pacific Investigations Review 2020*, a *Global Investigations Review* special report. *Global Investigations Review* is the online home for all those who specialise in investigating and resolving suspected corporate wrongdoing, telling them all they need to know about everything that matters.

Throughout the year, the *GIR* editorial team delivers daily news, surveys and features; organises the liveliest events ('GIR Live'); and provides our readers with innovative tools and know-how products. In addition, assisted by external contributors, we curate a range of comprehensive regional reviews – online and in print – that go deeper into developments than our journalistic output is able.

The *Asia-Pacific Investigations Review 2020*, which you are reading, is part of that series. It contains insight and thought leadership from 37 pre-eminent practitioners from the region. Across 16 chapters, spanning around 200 pages, it provides an invaluable retrospective and primer. All contributors are vetted for their standing and knowledge before being invited to take part.

Together, these contributors capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other articles provide valuable background so that you can get up to speed quickly on the essentials of a particular topic. This edition covers Australia, Cambodia, China, Hong Kong, India, Indonesia, Laos, Myanmar, Singapore, Thailand and Vietnam in jurisdictional overviews. It also looks at the impact of AI, data privacy, forensic accounting and law enforcement in multi-jurisdictional investigations.

If you have any suggestions for future editions, or want to take part in this annual project, we would love to hear from you.

Please write to insight@globalinvestigationsreview.com.

Global Investigations Review
London
August 2019

Data Privacy and Transfers in Investigations

Daniel P Levison, Sheryl J George, David Hambrick and Daniel Steel
Morrison & Foerster LLP

Increasing complexity and diversity among data privacy and data protection regimes in the Asia-Pacific region, together with the development of new regimes, have made conducting investigations in the region increasingly challenging. These legal frameworks may impose onerous restrictions on a company's ability to collect, transfer and disclose personal information, all of which are necessary to conduct internal investigations, to comply with subpoenas or requests for information from authorities, or where a company wishes to voluntarily disclose personal information to law enforcement agencies to obtain leniency. In particular, the US Department of Justice (DOJ), while acknowledging the complications companies face in these circumstances, views attempts by companies to resist disclosure of information on the basis of compliance with non-US data privacy laws with suspicion and places the burden on the company to show that the data privacy law in question prohibits disclosure.[1]

Bearing this context in mind, it is important that companies understand the requirements of the laws and regulations governing data privacy and data protection in the Asia-Pacific region.

Data privacy issues in the context of an investigation

The laws in most jurisdictions in the Asia-Pacific region permit the data protection authorities to impose significant penalties (both civil and criminal) for violations of data privacy laws and regulations. While the actual imposition of such penalties is uncommon, adherence to the applicable rules is critical at all relevant stages of an investigation.

1 FCPA Corporate Enforcement Policy, JM 9-47.120, 3.b, retrieved from www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.

Implementation of employment agreements and company data privacy policies

Companies must ensure that the routine collection, storage and use of employees' and customers' personal data comply with applicable data privacy laws and regulations. As discussed below, most jurisdictions require some form of notice, and in the employment context, a company's ability to collect and use personal data may often be prescribed by an employment agreement. Depending on local law and practice, this agreement may incorporate company policies on acceptable use of information technology resources, including the creation of personal data and the company's right to collect and use it. It is important that companies regularly review and update their employment agreements and company policies to keep up with legal and regulatory developments.

Companies should also consider company policies aimed to address the modes of communication employees use to conduct business. Many employees in the Asia-Pacific region use instant messaging applications; for example, WeChat is used routinely for business communications in China, and the same may be said of Line in Japan and elsewhere, KakaoTalk in Korea, and WhatsApp in many other locations around the region. The use of these messaging platforms poses challenges to securing the proper retention of business records, since these applications are not often maintained by the company. This frequently leads to the commingling of work-related and personal information because employees often use these messaging platforms on their personal devices, and the data generated by the platform may consequently be stored on the personal device or in a cloud-based account belonging to the employee. Some companies' IT-use policies strictly prohibit the use of these messaging platforms for business purposes; and others do not address it all. In light of the prevalence of these modes of communication, their importance as sources of potentially relevant information, and the risks of noncompliance with applicable data privacy laws and regulations, avoiding the issue is no longer tenable. Accordingly, it is important that companies clearly delineate how instant messaging platforms and personal devices may be used for company business and to what extent, if any, company-owned devices can be used for personal matters. This is for two overarching reasons: from a data privacy compliance perspective, the mixing of personal and work-related information significantly complicates the extraction of business information when it is needed for an investigation; and law enforcement agencies pay close attention to these issues.

In a notable development in March 2019, the DOJ revised provisions of its Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy, which sets out the conditions under which companies may seek leniency from the DOJ.[2] The revision included the introduction of new expectations for companies using instant messaging applications. The revision strongly encourages companies to ensure the implementation of 'appropriate guidance and controls' to secure the proper retention of business records. Where the original Policy (adopted in 2017) required companies to prohibit the use of 'software that generates but does not appropriately retain business records or communications', to secure full-cooperation credit in FCPA cases, the revised

2 Id., 9-47.120.

Policy now requires that companies demonstrate their ability to ensure the appropriate retention of business records and communications. While this appears to give companies some latitude to determine how this is done, companies will still need to determine what 'guidance and controls' are appropriate. The shift away from a blanket prohibition is a welcome step, particularly given the pervasive use of instant messaging applications in the conduct of business in the region. However, companies must still carefully assess their internal IT-use policies and evaluate if they are suitably robust in 'prohibiting the improper destruction or deletion of business records.'[3]

Collection of personal information

Personal information gathered during data collection or through interviews must comply with provisions requiring, for example, reasonable notice of the data that will be collected, the purposes for which the data is being collected, to whom the data may be disclosed, and, depending on applicable law, consent to the collection, use and possible disclosure. Of course, there may be other legal bases to process personal information, for example, to comply with a legal obligation, or to defend legal claims.[4]

Retention of personal data once it has been collected

Companies need to ensure that personal data is not kept for longer than the prescribed time limit under applicable law. This duty is sometimes complicated where routine deletion or non-retention of data may hamper an investigation, or conflict with regulations for preserving data in other jurisdictions. This issue frequently arises in FCPA investigations, where the DOJ sometimes views citing adherence to data privacy laws as an excuse for not disclosing information with scepticism.[5]

Cross-border transfer of data

Even where personal data does not leave a company's possession or control, if the company transfers the data across an international border, or if the data is accessed from outside the jurisdiction, that transfer or access may trigger provisions under data privacy laws that regulate whether and how that information can be transferred. For example, some jurisdictions, such as Australia, Japan and Singapore, impose a requirement on companies transferring data overseas to ensure that the data is afforded a standard of protection comparable to the standard of protection enjoyed in the jurisdiction where the data originated. China and Taiwan impose restrictions on cross-border transfers of certain categories of data for what appear to be protectionist

3 Id., 9-47.120, 3.c., 'The following items will be required for a company to receive full credit for timely and appropriate remediation... Appropriate retention of business records, and prohibiting the improper destruction or deletion of business records, including implementing appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations...'

4 See eg, Singapore's Personal Data Protection Act, Schs. 2–4; Australia's Privacy Act 1988, section 16A(1).

5 Id., 9-47.120, 3.b.

reasons. In the cross-border investigations context, data may need to be accessed or exported for review and analysis by legal and technical experts (for example, for document review or computer forensics purposes), and eventually for production to law enforcement authorities.

Disclosure of personal data to public authorities

Many jurisdictions provide certain exceptions to data privacy and data protection requirements where companies are requested or ordered to disclose personal information in connection with investigations by authorities, or where companies voluntarily disclose information to cooperate with law enforcement. However, even in the above circumstances there may be restrictions on disclosure. Some countries require a disclosure in such circumstances to be limited to only what is necessary. In other cases, as noted above, there may be broad restrictions on cross-border transfers of certain categories of information. The United States has recognised the possible tension between requests and orders for information by US authorities and laws in other countries that may prevent disclosure of that information. Under the CLOUD Act (discussed in further detail below), a US digital service provider may resist disclosure of data to US authorities, even when served with orders or subpoenas, if the service provider reasonably believes: that the target of the request is not a US person and does not reside in the United States; and that the required disclosure creates a material risk that the service provider would violate the laws of another country with which the US government has an executive agreement under the CLOUD Act.

Appreciating how data privacy and data protection issues may arise under various countries' laws at different stages of an investigation will help companies to appropriately address such issues, especially in complex multi-jurisdictional investigations, and to avoid potential violations that may interfere with the conduct of an investigation or result in severe penalties.

Data privacy regimes in the Asia-Pacific region

Core principles of data protection

Generally, laws of the countries in the Asia-Pacific region with established data privacy and data protection regimes require that individuals be informed of what personal information is collected, why it is collected and with whom it is shared. Although the mechanisms differ by jurisdiction, there are several common principles:

- Notice: individuals must be informed in advance what information will be collected, how it will be used and to whom it will be disclosed.
- Consent: individuals often must be afforded some type of consent or choice regarding the use and sharing of their information.
- Data security: companies that collect, use and disclose personal information must take reasonable precautions to protect that information from loss, misuse, unauthorised access, disclosure, alteration and destruction.
- Access and correction: individuals must be able to access and, where appropriate, correct, update or suppress information collected about them.

- Data integrity: companies that collect personal information must take steps to ensure that it is accurate, complete and up to date.
- Data retention: companies must only retain personal information for the period of time it is required.

Established versus evolving data privacy regimes

Many jurisdictions in the Asia-Pacific region have comprehensive and established data privacy and data protection laws, including Australia, Hong Kong, India, Japan, Macao, Malaysia, New Zealand, the Philippines, Singapore, South Korea, Taiwan and, most recently, Thailand.[6] These jurisdictions have generally adopted laws and regulations putting into effect the core principles of data protection discussed above. Indonesia has also moved towards establishing a more comprehensive regime, with its introduction of Ministry of Communication Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems on 1 December 2016, although many principles of data privacy and data protection have not yet been fully developed.

Other jurisdictions in the Asia-Pacific region without comprehensive or consolidated privacy laws, including China and Vietnam, are moving towards development of data privacy and data protection laws at different rates and in different ways.

China

The body of law in China that touches on issues of data privacy and data protection is contained in a multitude of legislation, including the General Rules of Civil Code, the Tortious Liability Law, the Criminal Law, the Consumer Protection Law, and the Standing Committee of China's National People's Congress Decision on Network Information Protection dated 28 December 2012. On 1 June 2017, the Cybersecurity Law came into force, significantly developing the law regarding data protection and transfer.

The Cybersecurity Law governs a wide range of technology- and network-related issues, as well as the protection and transfer of personal information. The law imposes far-reaching restrictions on how computer networks are to be operated. Two noteworthy features of the law are the requirement of data localisation, and some heavy-handed restrictions on cross-border data transfer, which are discussed below.

On 1 May 2018, China's National Information Security Standardisation Technical Committee issued an amended version of China's GB/T 35273-2017 – Information Security Technology – Personal Information Security Specification, known as China's 'Privacy Standard'. The Privacy Standard sets out the best practices for the collection and processing of personal information and, while not technically binding, is generally used to assess companies' compliance with

6 In the previous edition of this article, we noted that Thailand was in the process of introducing a comprehensive privacy regime under the Thai Personal Data Protection Bill that contained many of the common core principles of privacy regimes found in other jurisdictions in the Asia-Pacific region. On 28 February 2019, the Thai National Legislative Assembly approved and endorsed the bill, which became the Thai Personal Data Protection Act. The act was given royal assent and was subsequently published in the Thai Government Gazette on 27 May 2019. Applicable business operators In Thailand have until 27 May 2020 to become fully compliant with the new law.

China's data protection laws and rules. Most recently, on 21 May 2019, the China Administration of Cyberspace issued a draft regulation for public comment, titled 'Measures on Cybersecurity Review', which, if implemented, would further develop the data privacy landscape in China.

Vietnam

In Vietnam, there is no consolidated law on data privacy. The laws touching on these issues are found in multiple documents, including the Constitution, the Civil and Criminal Codes, the Consumers' Rights Protection Law, the E-Commerce Law, the Law on Information Technology, the Law on Network Information Security and the Law on Cybersecurity. Together, however, these laws provide protection roughly in accordance with the core principles highlighted above.

Relevant features of Asia-Pacific data privacy regimes in the context of investigations

Data privacy and data protection regimes in the Asia-Pacific region vary to some degree in their approaches. Important differences among the regimes relevant to the conduct of an investigation relate mainly to: the role an individual's consent plays in the collection, use and disclosure of personal information; a company's obligation to retain personal information for a limited period of time; and the manner in which personal data can be disclosed or transferred across international borders.

The requirement to obtain consent

While some Asia-Pacific jurisdictions impose a requirement to obtain an individual's consent before personal data is used or transferred, the same requirement does not necessarily apply equally in all jurisdictions with respect to the collection of personal data. For instance, in Australia, there is no requirement for organisations to obtain an individual's consent to collect information; entities need only ensure that the collection of the information is reasonably necessary for one or more of the organisation's functions or activities.[7] Consent does play a role in Australia, however, where an organisation wishes to use or disclose personal information for a different reason than that for which it was collected.[8] Hong Kong has adopted this same approach to the question of consent.[9]

Many jurisdictions, however, do require that entities obtain the consent of the individual before personal information about that individual is collected. In Singapore, organisations may only collect, use or disclose personal data for the purposes for which an individual has given consent,[10] although several exceptions to this general rule apply. For example, Singapore provides exceptions to the requirement of obtaining consent in the context of investigations,

7 Australia's Privacy Act 1988, Sch. 1, cl. 3.

8 Id., Sch. 1, cl. 6.

9 Hong Kong's Personal Data (Privacy) Ordinance (Cap. 486), Sch. 1 para. 1.

10 Singapore's Personal Data Protection Act 2012, section 13.

but only where the collection, use or disclosure is necessary, with an additional requirement for collection that it must be reasonable to expect that seeking consent would compromise the availability or accuracy of the personal data in question.[11]

In Japan, the position is more nuanced. Where the data is considered to be sensitive personal information – as opposed to merely personal information – the business operator in question is required to obtain the individual's consent to collect the data;[12] where the information is not considered sensitive, Japanese law simply provides that the information must not be acquired through deception or other wrongful means.[13] The term 'sensitive personal information' is defined as information specified by the Japanese authorities as requiring special consideration in handling to avoid any unfair discrimination, prejudice or other disadvantage to an individual based on the person's race, creed, social status, medical history or criminal records, or the fact that a person has incurred damages through an offence.[14] Japanese privacy law provides an exception to the requirement to obtain consent for collection of personal data where such collection is needed to cooperate with public authorities and obtaining the individual's consent is likely to interfere with the public authorities' affairs.[15] This exception also applies to the disclosure of personal data to a third party.[16] This exception does not extend to internal investigations, however.

Under Taiwanese law, consent is not treated as a requirement, but rather as one of many conditions that may justify collection and processing of personal data. To comply with privacy law, data collection by Taiwanese data collectors and processors must meet one of the prescribed conditions in article 19 of the Taiwan Personal Data Protection Law, as well as be for a specified purpose.[17]

Other countries in the region that impose some type of consent requirement for the collection of personal data include China, Indonesia, Malaysia, the Philippines, Thailand and Vietnam.

Retention of personal data

Jurisdictions in the Asia-Pacific region, such as Australia, Hong Kong, Japan, Malaysia, the Philippines, Singapore, Taiwan, Thailand and Vietnam generally do not specify time limits for the retention of data, but instead provide that, once the purpose for which the personal data were collected has been exhausted, the entity in question should cease to retain the information in question. A recent example of this is found in Vietnam's Law on Cybersecurity, which came into effect on 1 January 2019. Under the new law, domestic and foreign companies providing telecommunications, internet and cyberspace services in Vietnam are required to store personal

11 Id., Sch. 2 para. 1(e), Sch. 3 para. 1(e), Sch. 4 para. 1(f).

12 Japan's Act on the Protection of Personal Information, article 16(1).

13 Id., article 17(1).

14 Id., article 2(3).

15 Id., article 17(2)(iv).

16 Id., article 23(1)(iv).

17 Taiwan's Personal Data Protection Act, article 19(5).

information for as long as the company continues to provide the services in question. In other countries (such as China and Indonesia), general bookkeeping laws and regulations relating to the archiving of data apply to the retention of personal information.

A tension may exist between local privacy law requirements for the retention and eventual destruction of personal information, and requirements or conditions imposed by government regulators and authorities when conducting investigations. As discussed above, the DOJ views attempts by companies to resist disclosure of information on the basis of compliance with non-US data privacy laws with suspicion. Under the DOJ FCPA Corporate Enforcement Policy, some of the factors that the DOJ considers when determining whether to exercise leniency are whether there was: (1) 'timely preservation, collection and disclosure of relevant documents and information relating to their provenance'; and (2) 'appropriate retention of business records, and [prohibition of] the improper destruction or deletion of business records.'[18] In respect of the first factor, the DOJ notes that where a company claims that disclosure of overseas documents is prohibited by reason of local data privacy laws, the burden is on the company to establish such prohibition.[19]

Therefore, in FCPA investigations at least, where proper disclosure of personal information cannot be completed because of data privacy laws governing the retention and destruction of such information, companies must be able to demonstrate that the non-retention or destruction of the data in question was done pursuant to and in accordance with mandatory laws governing data retention.

Cross-border disclosures and transfers of personal data

Rules for cross-border disclosures and transfers differ greatly among countries in the Asia-Pacific region. In general, the entity sending personal data overseas must ensure that the recipient entity or country provides protection of personal information in a materially similar manner to the jurisdiction from where the data was sent, but this requirement is not universally applicable. Where there is such a requirement, many Asia-Pacific data privacy and data protection regimes do not generally provide guidance on which countries are deemed to provide adequate protection. A way for companies to mitigate the risks of violating these requirements when transferring data cross-border is by entering into contractual arrangements designed to adhere to a standard of data protection more closely aligned with the laws of the country where the data was initially created.

In Australia, where an entity discloses personal data to a recipient abroad, the entity sending the information must take reasonable steps to ensure that the overseas entity does not breach the Australian Privacy Principles set out in Schedule 1 of Australia's Privacy Act 1988.[20] If the overseas entity breaches the Australian Privacy Principles (APPs), then the entity sending the information is taken as having breached those principles itself.[21] However, exceptions exist, for

18 FCPA Corporate Enforcement Policy, JM 9-47.120, 3.b.

19 Id.

20 Australia's Privacy Act 1988, Sch. 1, sub-cl. 8.1.

21 Id., section 16C.

example, if the entity sending the data reasonably believes that the recipient entity is subject to a data privacy regime that is materially similar to the position under Australian law, or where the individual consents to the transfer of his or her data (where the individual has been expressly informed by the sending entity that, if he or she consents to the overseas disclosure of the information, the entity will not be required to take reasonable steps to ensure the overseas recipient does not breach the APPs).[22] Where the entity in question is a governmental agency, there are two additional exceptions that may apply: the agency may make the disclosure where it is required by an international agreement relating to information sharing to which Australia is a party; and where the entity believes that the cross-border transfer is reasonably necessary for an enforcement action.[23]

Japan imposes restrictions that are similar to those in Australia. In addition to the condition that the individual in question must provide his or her consent, Japan also permits the transfer of personal information overseas if: (1) the recipient entity has a system in place deemed compliant with the data protection standards under Japanese law; or (2) the recipient is located in a country with a data privacy regime deemed equivalent to the Japanese regime, as designated by Japan's Personal Information Protection Commission.[24] Malaysia and Singapore have also adopted similar restrictions on cross-border data transfers.

Some other countries have introduced aspects of protectionism in their restrictions on cross-border data transfers. For example, under Taiwan's Personal Data Protection Law, where a non-governmental entity seeks to transmit personal information overseas, Taiwanese regulators may prevent transmission where such transmission is in respect of personal information that involves major national interests.[25]

The most critical example of this type of transfer restriction is found in China's new Cybersecurity Law. The law provides that operators of critical information infrastructure (CII Operators), must undergo a security assessment before information can be moved cross border.[26] CII Operators are operators of certain major computer networks, which include networks relating to public communications and information services, energy, finance, transportation, water conservation, public services and e-governance.[27] Although China has released guidance on what it considers to be sectors with critical information infrastructure,[28] which may be instructive in understanding what is considered a CII Operator under the Cybersecurity Law, it is still unclear whether companies that operate in one of the identified sectors are automatically considered CII Operators. It is also not clear at present what the required security assessment

22 Id., Sch. 1, sub-cl. 8.2(a)(i)–(ii), 8.2(b)(i)–(ii).

23 Id., Sch. 1, sub-cl. 8.2(e), 8.2(f)(i)–(ii).

24 Japan's Act on the Protection of Personal Information, article 24.

25 Taiwan's Personal Data Protection Act, article 21.

26 China's Cybersecurity Law, article 37.

27 China's Cybersecurity Law, article 31.

28 China's National Network Security Inspection Operational Guide, section 3.2; China's Regulations on the Security Protection of Critical Information Infrastructure, article 18.

will entail, as China's cyberspace administration bodies are still in the process of developing assessment measures. What is apparent, however, is that cross-border transfers of data by CII Operators will become much more cumbersome.

The APEC privacy framework: moving towards harmonisation?

The Asia-Pacific Economic Cooperation (APEC) is a regional forum made up of 21 economies that seeks to secure growth and accelerate regional economic integration. Two APEC initiatives aim to harmonise standards for privacy and data protection around the Asia-Pacific region: the Cross-Border Privacy Rules (CBPR) System is a voluntary system for facilitating the exchange of personal information among participating APEC economies; and the Privacy Recognition for Processors (PRP) System is a set of requirements intended to help personal information processors comply with relevant privacy obligations. The CBPR and PRP establish baseline protections but do not alter domestic laws.

Although all 21 APEC jurisdictions have endorsed the CBPR System, to participate, each must officially express its intent to join and meet requirements. There are currently eight participating APEC CBPR economies: Australia, Canada, Chinese Taipei (ie, Taiwan), Japan, Mexico, Singapore, South Korea and the United States. As at the time of writing this article, 28 companies have also been certified under the CBPR System by demonstrating compliance to an APEC CBPR-recognised accountability agent.

Singapore and the United States also participate in the PRP System by demonstrating compliance with its baseline requirements for data protection to the APEC Joint Oversight Panel. The Philippines and Taiwan have also submitted notices of their intention to join the CBPR and PRP Systems in the near future.

Additional development to watch: influence of the GDPR

The European Union General Data Protection Regulation (GDPR) intends to strengthen and harmonise data protection laws within the EU and regulate export of personal data. Unlike the APEC CBPR System, the GDPR is directly binding on organisations. The GDPR's influence in Asia-Pacific jurisdictions was apparent even before it became effective in May 2018; the GDPR applies to organisations that are established outside the EU but that offer goods or services to individuals in the EU or that monitor behaviour of individuals, where the behaviour takes place in the EU. As a result, if a company located in the Asia-Pacific region were to conduct an investigation of its own EU-based staff by means that monitored their behaviour, the Asia-Pacific-based company could fall within the GDPR's extraterritorial provisions and, therefore, be required to comply with the GDPR in relation to the monitoring.

Noting the GDPR's likely impact on non-EU businesses as a result of its extraterritoriality, Hong Kong's Privacy Commissioner for Personal Data (PCPD) has advised and promoted GDPR compliance. The PCPD has also issued a publication to raise awareness among businesses in Hong Kong of the possible impact of the new regulatory framework for data protection in the

GDPR and to assist them in understanding the major disparities in view of the extraterritorial application of the GDPR, as well as comparing some of the major requirements with those set out in Hong Kong's Personal Data Privacy Ordinance.[29]

Similarly, when the Philippines developed implementing rules and regulations for the country's first comprehensive data protection law, it sought to harmonise with the European approach by including a right to object to profiling, a right to data portability and a mandatory 72-hour data breach notification requirement.

Most recently, on 23 January 2019, the EU and Japan adopted an agreement to create the world's largest area of safe data flow, recognising each other's data protection systems as equivalent.[30] The agreement covers 'personal data exchanged for commercial purposes, ensuring that in all exchanges a high level of data protection is applied.'[31] The agreement also requires Japan to implement a set of rules providing individuals in the EU whose personal data is transferred to Japan with additional safeguards to address certain differences between the two systems and to implement a complaint-handling mechanism to investigate and resolve complaints from Europeans regarding Japanese authorities' access to their personal data. After two years, the first joint review will assess the functioning of the framework. Subsequently, a review will take place at least every four years.

Additional development to watch: the CLOUD Act

Historically, in the context of investigations and law enforcement, government regulators and investigators have faced significant problems with retrieving personal data that is stored outside their jurisdiction.

US lawmakers have attempted to address this problem. In March 2018, President Trump signed the CLOUD Act into law, requiring certain US digital service providers that are served with court orders under the Stored Communications Act to turn over data no matter where stored, so long as it is within the US company's 'possession, custody, or control'. A second feature of the CLOUD Act is the regime permitting regulators of countries that have signed an executive agreement with the United States to request documents directly from US companies as long as the US digital service provider is subject to the jurisdiction of that foreign government. The CLOUD Act will thus substantially expand the power of investigators and regulators to retrieve data and documents from companies and data centres, wherever they are in the world.

This means that all data – personal data included – is now potentially more accessible to US authorities and countries with which the US has entered into an executive agreement under the CLOUD Act. This is important in the Asia-Pacific context, not least because, over the past few years, large US companies and cloud service providers have established data centres in key

29 Office of the Privacy Commissioner for Personal Data, "European Union General Data Protection Regulation (GDPR) 2016," available at: www.pcpd.org.hk/english/data_privacy_law/eu/files/eugdpr_e.pdf.

30 European Commission, (23 January 2019), Safe Data Flows Between EU and Japan [Press release], retrieved from https://ec.europa.eu/unitedkingdom/news/safe-data-flows-between-eu-and-japan_en.

31 European Commission, (17 July 2018), The European Union and Japan agreed to create the world's largest area of safe data flows [Press release], retrieved from http://europa.eu/rapid/press-release_IP-18-4501_en.htm.

jurisdictions in the region,[32] meaning that the United States may wield more power to compel production of personal information that was created in Asia and that is held by US cloud service providers.

Conclusion

Conducting an effective internal investigation and responding to requests and orders from authorities in connection with regulatory investigations are complicated by a company's need to comply with applicable data privacy and data protection laws. These complications are particularly evident in the Asia-Pacific region, where the data privacy and data protection framework is heavily fragmented and approaches to data privacy and data protection are so diverse. Although there have been some efforts to harmonise the applicable principles, these efforts fall far short of creating a uniform system of personal data protection. Companies must appreciate the nuances of applicable data privacy rules in each country and how they might affect the conduct of an internal investigation or the scope of their obligations to respond to requests or orders from applicable law enforcement authorities.

32 See, eg, Visa, (26 July 2017), Visa Expands Global Transaction Processing with Facilities in Singapore and United Kingdom [Press release], retrieved from http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=2288776; LinkedIn, (6 April 2016), LinkedIn's first data centre outside of the US comes online in Singapore [Press release], retrieved from https://news.linkedin.com/2016/linkedins-first-data-centre-outside-of-the-US-comes-online-in-Singapore; Kava, J, Google Vice President of Data Centers, (2 June 2015), Growing our data centre in Singapore, retrieved from https://blog.google/topics/google-asia/growing-our-data-center-in-singapore/.

Daniel P Levison
Morrison & Foerster

Daniel Levison is a partner in Morrison & Foerster's Singapore office, where he heads its litigation department. Mr Levison counsels clients regarding compliance matters and conducts internal investigations and compliance reviews across the Asia-Pacific region, where he has over 19 years of experience.

Clients say that Mr Levison 'is intelligent, thorough and flexible in meeting our companies' needs', and they rely on his experience with highly sensitive matters, which have included fraud and corruption, cartel and other competition matters, anti-money laundering, export control, privacy and data security, and regulatory and product safety investigations. In addition, he assists clients with pre-acquisition and third-party anti-corruption due diligence, and developing, reviewing and implementing anti-corruption policies, procedures and training programmes.

Mr Levison also focuses on complex commercial litigation and arbitration matters, with particular emphasis on the resolution of multi-jurisdictional disputes, and he has developed particular expertise regarding cross-border electronic discovery matters. Mr Levison has counselled clients in a range of matters involving contract disputes, business torts, antitrust, product liability, intellectual property and other issues.

Mr Levison was recently listed by *Chambers Asia-Pacific 2018* and *2019*, as well as *Who's Who Legal: Investigations 2019*, as a top practitioner in his field for corporate investigations and anti-corruption.

Sheryl J George
Morrison & Foerster

Sheryl George is a disputes and compliance associate in the Singapore office of Morrison & Foerster. Her practice focuses on investigations and white-collar matters, regulatory and global compliance, including compliance due diligence for corporate transactions, as well as complex commercial disputes. Ms George has particular expertise in fraud and corruption, money laundering, economic sanctions, cybercrime and cybersecurity, and a broad range of complex commercial matters.

Prior to joining Morrison & Foerster, Ms George was a deputy public prosecutor/state counsel in the Criminal Justice Division, Financial and Technology Crime Division, and the Advocacy Group of the Singapore Attorney-General's Chambers, where she served as the lead prosecutor and state counsel on a wide variety of financial crime and regulatory matters, and successfully argued a number of cases before the High Court of the Republic of Singapore.

Ms George received her Bachelor of Laws from University College London (UCL), and her Master of Laws in international legal studies from New York University (NYU) School of Law. She participated in the Philip C Jessup International Law Moot Court Competition teams at both UCL and NYU. Ms George is admitted to the bar in Singapore and New York, and is a registered foreign lawyer in Singapore. She is fluent in English and Bahasa Melayu, and conversant in Malayalam.

David Hambrick
Morrison & Foerster

David Hambrick is a disputes and compliance associate in Morrison & Foerster's Singapore office. He advises and represents clients in multi-jurisdictional investigations, regulatory matters, and compliance reviews involving financial institutions and global companies.

Mr Hambrick's practice also includes high-value international arbitration proceedings and complex litigations, with a particular focus on energy, insurance, construction, joint ventures, sovereign wealth funds and general commercial disputes.

Mr Hambrick regularly provides transactional and pre-dispute advice to clients on a wide range of issues such as the construction of arbitration clauses in commercial contracts, third-party funding, risk analysis and mitigation, and sovereign immunity.

Prior to joining Morrison & Foerster, Mr Hambrick was an international arbitration and litigation associate in the London, Paris and New York offices of another leading international law firm. He served as a law clerk to the Honorable Andrew J Peck of the US District Court for the Southern District of New York in 2009.

Mr Hambrick received his JD from Columbia Law School, where he was a Harlan Fiske Stone Scholar, recipient of the Parker School Certificate for Achievement in International and Comparative Law, and editor-in-chief of the Columbia Journal of Transnational Law. He received his AB from Harvard University. He is admitted to the New York Bar.

Daniel Steel
Morrison & Foerster

Daniel Steel is a disputes and compliance associate in the Singapore office of Morrison & Foerster. He assists clients with conducting internal investigations and the implementation of compliance policies and programmes, including with respect to white-collar criminal matters, and those in connection with the US FCPA. He also advises clients on complex commercial disputes, with a particular focus on international commercial arbitration matters. His practice and experience span a wide variety of industry sectors including construction, oil and gas, telecommunications, securities, medical and pharmaceuticals, among others. He has conducted numerous arbitrations under the SIAC, ICC and UNICTRAL arbitral rules.

Prior to joining Morrison & Foerster, Mr Steel worked in the white-collar crime and international arbitration departments of a leading international law firm in both its New York and Singapore offices.

Mr Steel received his Bachelor of Arts (Hons) (Law) from Magdalene College, University of Cambridge, and his Master of Laws in international legal studies from Georgetown University Law Center.

Mr Steel is admitted to practise law in New York. He is fluent in both English and Norwegian, and proficient in Mandarin Chinese and French.

MORRISON FOERSTER

Morrison & Foerster is a leading international law firm with over 35 years of experience in Asia. Strategically located in major financial centres in China, Japan and Singapore, the firm's disputes and investigations practice handles all types of complex, multi-jurisdictional litigation, international arbitration, intellectual property, compliance and investigations matters (including FCPA/anti-corruption, securities litigation, white-collar/investigation and enforcement). With over 50 disputes specialists, it is one of the largest in the region.

The firm's investigations and compliance practice delivers a unique set of global and regional capabilities. Extensive trial experience before courts, administrative agencies and arbitral tribunals around the globe equips the team to manage the full life cycle of matters, comprising strategy, case management and advocacy. Its fully integrated and diverse team includes leading trial lawyers, former US federal prosecutors, senior government policy makers, privacy experts, forensic accountants, fraud examiners and local experts. Through its network of 17 offices across Asia, Europe and the United States, Morrison & Foerster has advised companies and individuals on anti-corruption and compliance matters in more than 140 countries.

The firm's lawyers on the ground in Asia have experience across all types of investigations and regulatory compliance issues faced by global companies operating in the region, including:

- Anti-corruption
- Antitrust/cartel
- Anti-money laundering and fraud
- Global risk and crisis management
- Data privacy/cybersecurity
- Export controls and sanctions
- Internal investigations

The Asia-based team includes lawyers from Singapore, Japan, Hong Kong, China, the UK, New Zealand and the United States, and provides multilingual language capability in English, Mandarin, Cantonese and Japanese.

50 Collyer Quay
12-01 OUE Bayfront
Singapore 049321
Tel: +65 6922 2000
Fax: +65 6922 2008

www.mofo.com

Daniel P Levison
dlevison@mofo.com

Sheryl J George
sgeorge@mofo.com

David Hambrick
dhambrick@mofo.com

Daniel Steel
dsteel@mofo.com

The *Asia-Pacific Investigations Review 2020* contains insight and thought leadership from 37 pre-eminent practitioners from the region. Across 16 chapters, spanning around 200 pages, it provides an invaluable retrospective and primer.

Together, these contributors capture and interpret the most substantial recent international investigations developments of the past year, with footnotes and relevant statistics. Other articles provide valuable background so that you can get up to speed quickly on the essentials of a particular topic. This edition covers Australia, Cambodia, China, Hong Kong, India, Indonesia, Laos, Myanmar, Singapore, Thailand and Vietnam in jurisdictional overviews. It also looks at the impact of AI, data privacy, forensic accounting and law enforcement in multi-jurisdictional investigations.

Visit globalinvestigationsreview.com
Follow @GIRAlerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-225-1