Volume 4 Number 3 2021 ISSN 2398-1679

Journal of Data Protection & Privacy

Henry Stewart Publications
Ruskin House, 40-41 Museum Street,
London, WC1A 1LT, UK
Tel: +44 (0)20 404 3040
Website: www.henrystewartpublications.com

Henry Stewart Publications
North American Business Office
The Bleachery
143 West Street
New Milford, CT 06776, USA
Tel: +1 860 350 0041; Fax: +1 860 350 0039
e-mail: hsp@subscriptionoffice.com

ISSN 2398-1679

Printed in the United Kingdom by Charlesworth Press, Wakefield, UK

Journal of Data Protection & Privacy has been accepted for inclusion in the abstract and citation database, Scopus.

Contents

Practice papers

China's draft Personal Information Protection Law

Received: 19th April, 2021

Lothar Determann
Baker McKenzie, San Francisco

Lothar Determann teaches computer, internet, data privacy and commercial law at Freie Universität Berlin, University of California, Berkeley School of Law and Hastings College of the Law, San Francisco, and practices law as a partner at Baker McKenzie, where he has been counselling companies since 1998 on privacy law compliance and taking products and business models international. He has authored numerous articles, treatise contributions and books, including *Determann's Field Guide to Data Privacy Law* and *California Privacy Law — Practical Guide and Commentary*.

Two Embarcadero Center, Suite 1100, San Francisco, California 94111, USA
Tel: +1 (650) 856-5533; E-mail: Lothar.Determann@bakermckenzie.com

Zhenyu (Jay) Ruan
Baker McKenzie FenXun (FTZ) Joint Operation Office, China

Zhenyu (Jay) Ruan specialises in corporate and regulatory advisory matters in China. He is a member of Baker McKenzie's Global TMT Steering Committee, making him instrumental in the TMT space for China and the whole of Asia Pacific. He has advised on significant deals which include technology companies' joint ventures and technology licensing transactions, e-commerce and data privacy matters for multi-national fashion and retail and healthcare companies, and regulatory and cybersecurity law for financial institutions and technology companies.

Unit 1601, Jin Mao Tower, 88 Century Avenue, Pudong, Shanghai 200121, PRC
Tel: +86 21 6105 8577; E-mail: Zhenyu.Ruan@bakermckenziefenxun.com

Tingting Gao
Baker McKenzie FenXun (FTZ) Joint Operation Office, China

Tingting Gao is an associate at Baker McKenzie, primarily focusing on China-related corporate, regulatory and compliance advisory matters, with an expertise in data privacy and cybersecurity. She has advised clients from a wide range of sectors with their data privacy and cybersecurity compliance in China. She is admitted to practice in PRC (inactive) and New York.

Unit 1601, Jin Mao Tower, 88 Century Avenue, Pudong, Shanghai 200121, PRC
Tel: +86 21 6105 5910; E-mail: Tingting.Gao@bakermckenziefenxun.com

Jonathan Tam
Baker McKenzie, San Francisco

Jonathan Tam is a senior associate at Baker McKenzie focusing on global privacy, technology transactions and cybersecurity. He started in Baker McKenzie's Toronto office in 2012 and transferred to the firm's San Francisco office in 2018. He is a co-chair of the IAPP's Silicon Valley KnowledgeNet chapter and a member of the Executive Committee of the San Francisco Bar Association's Privacy and Cybersecurity Section.

Two Embarcadero Center, Suite 1100, San Francisco, California 94111, USA
Tel: +1 (415) 984-3883; E-mail: Jonathan.Tam@bakermckenzie.com

Abstract In October 2020, China published a draft of the Personal Information Protection Law of the People's Republic of China (PRC) for public comment. The draft law is intended to be the first consolidated and comprehensive law targeting the protection of personal information in China. If enacted in its current form, the law would introduce a suite of obligations that apply to organisations in both the private and public sectors and individuals that process Chinese residents' personal information. The scope, structure and substance of the draft law not only resemble that of the European Union (EU) General Data Protection Regulation (GDPR) in a number of key ways but also diverge from the GDPR in many respects. The draft Chinese law also has some similarities with various US privacy laws, although the United States has not enacted a comprehensive federal privacy law that applies across the country. Despite the variations among the regimes of China, the EU and the United States, organisations that do business in these geographies can leverage the privacy compliance programmes they may have established for the United States and EU to prepare for the implementation of the draft Chinese Personal Information Protection Law. This paper summarizes the key requirements of the draft Chinese law and provides high-level observations regarding its similarities to and differences from the GDPR and key US privacy laws.

KEYWORDS: China, PRC, Personal Information Protection Law of the PRC, PRC Cybersecurity Law, PRC Data Security Law, Chinese privacy laws, Cyberspace Administration of China, comparative analysis, EU General Data Protection Regulation, California Consumer Privacy Act, Virginia Consumer Data Protection Act, US Health Insurance Portability and Accountability Act

INTRODUCTION

On 21st October, 2020, China published a draft of the Personal Information Protection Law of the PRC (Draft PRC Personal Information Protection Law) for public comment. In this paper, the terms 'China' and 'PRC' refer to the People's Republic of China, excluding the Hong Kong and Macau Special Administrative Regions and Taiwan, which the personal information protection regime in China regards as foreign jurisdictions. The term 'Chinese' refers to China only. The Draft PRC Personal Information Protection Law is intended to be the first consolidated and comprehensive law targeting the protection of personal information in the country. If enacted in its current form, the law would introduce a suite of obligations that apply to organisations in both the private and public sectors and individuals that process Chinese residents' personal information. There is no clear timeline for the implementation of the statute, but it is widely expected to take place in late 2021 or sometime during 2022.

The scope, structure and substance of the Draft PRC Personal Information Protection Law resemble that of the European Union (EU) General Data Protection Regulation (GDPR) in a number of key ways. For example, both instruments set forth similar conditions in which they would apply extraterritorially, distinguish between controllers and processors, require foreign controllers to designate a local representative, set hefty administrative fines measured in proportion to the yearly turnover of an institutional offender, impose heightened requirements regarding the processing of sensitive personal information and establish certain fundamental rights of individuals to whom personal information pertains. However, the draft Chinese law also diverges from the GDPR in many respects. For example, the Draft PRC Personal Information Protection Law does

not specify the pursuit of legitimate interests as a lawful basis of processing, lists more circumstances than the GDPR does in which a controller must conduct a security assessment (similar to a data protection impact assessment under Article 35 of the GDPR), does not provide individuals with a right to data portability, imposes data residency requirements on certain types of controllers and sets different requirements regarding cross-border transfers of personal information.

Similar to the Draft PRC Personal Information Protection Law, Brazil and India,[1] several US states have started to adapt principles and provisions from the GDPR, including California (with the California Consumer Protection Act of 2018, as amended by the California Privacy Rights Act of 2020 [collectively, CCPA])[2] and Virginia (with the Virginia Consumer Data Protection Act [VCDPA]).[3] These US state laws and the earlier US Health Insurance Portability and Accountability Act of 1996 and related regulations, as amended (collectively, HIPAA), which may have inspired the GDPR, give individuals the right to access and correct the personal information that businesses hold about them and codify certain foundational privacy principles,[4] including that organisations should not process more personal information than necessary to fulfil the purposes for which they were collected. On a federal level, the United States has not so far followed the EU approach of comprehensively regulating the processing of personal data. Instead, the United States has traditionally enacted industry-, harm- and activity-specific privacy laws, such as HIPAA, which focuses on the healthcare and health insurance industry. The CCPA and VCDPA only protect residents of their respective state and only apply to certain types of activities in the private sector. The passage of the Draft PRC Personal Information Protection Law would therefore further distinguish the Chinese personal information protection regime from that of the United States.

Despite these variations, organisations can leverage the privacy compliance programmes they have established for the United States and EU to prepare for the implementation of the Draft PRC Personal Information Protection Law. For instance, organisations can:

- Leverage internal processes, protocols and resources related to responding to data subject requests to build out a data subject request response mechanism for China;
- Extend special consent and data handling procedures to the processing of sensitive personal information of Chinese residents and minors residing in China;
- Maintain and document appropriate technical, organisational and physical privacy and security measures for China, including by performing due diligence of vendors, managing vendor agreements, monitoring vendor compliance and administering regular data privacy and security training for personnel;
- Build on internal processes relating to data protection impact assessments and data breach reporting to account for new Chinese requirements;
- Use much of the same substance of their existing privacy notices potentially to address notice requirements under the draft Chinese law;
- Make use of existing binding corporate rules and intra-group data processing agreements to document the outward provision of personal information of Chinese residents from China to other jurisdictions;
- Implement organisation-wide data minimisation and deletion requirements as appropriate and
- Ensure that management continues to support privacy compliance efforts and an accountability framework that extends to China.

This paper focuses on the current personal information protection regime in China and how the Draft PRC Personal Information Protection Law would change it. Section 1 outlines the overall regulatory framework within which the Draft PRC Personal Information Protection Law exists. Section 2 identifies the regulatory agencies that enforce Personal Information Protection Laws in China. Sections 3–10 outline in greater detail the requirements under China's Personal Information Protection Laws and Section 11 elaborates on the sanctions and penalties that may apply in the event of noncompliance. This paper includes some high-level observations regarding significant differences and similarities between China's Personal Information Protection Laws and EU and US laws, but a comprehensive comparative analysis is beyond its scope.

LEGAL AND REGULATORY FRAMEWORK FOR THE PROTECTION OF PERSONAL INFORMATION OF INDIVIDUALS

The Chinese legislature plans to establish legal regimes that will apply to the following three core areas: (i) network (cyber) security; (ii) the protection of personal information of individuals and (iii) the security of data other than personal information. Three basic laws (ie foundational codes) and their respective implementing measures, rules and guidelines will regulate these three areas. Currently, the basic law governing network (cyber) security has been enacted and is in effect. The Draft PRC Personal Information Protection Law would govern the protection of personal information. A third basic law would apply to the security of data other than personal information.

PRC Cybersecurity Law

The Cybersecurity Law of the PRC (PRC Cybersecurity Law) became effective on 1st June, 2017, and establishes general requirements regarding the construction, operation, maintenance, use and security of networks in China. The PRC Cybersecurity Law defines 'network (cyber)' broadly as 'a system that consists of computers or other information terminals and relevant devices and serves to collect, store, transmit, exchange and process information per certain rules and procedures'.[5] This is a broad definition that may encompass internet-connected networks, intranets, local area networks and other forms of networks. The PRC Cybersecurity Law applies to 'network operators', which the law defines as 'owners and administrators of networks as well as network service providers'.[6] The statute imposes various requirements on network operators, including the data residency and security assessment requirements outlined in the sections 'Are there data residency requirements in China?' and 'Under what circumstances must an entity perform a security assessment in China?' later in this paper, respectively. The PRC Cybersecurity Law also establishes certain key principles, concepts and rules concerning the protection of personal information and other non-personally identifiable data, which serve as important foundations for the other two basic laws.

Draft PRC Personal Information Protection Law

The Draft PRC Personal Information Protection Law is a milestone in China's efforts to consolidate the bulk of personal information protection requirements in a single piece of legislation. This paper elaborates on the Draft PRC Personal Information Protection Law in the following sections.

Draft PRC Data Security Law

On 3rd July, 2020, China released the draft Data Security Law of the PRC (Draft PRC Data Security Law) to solicit public comments. The Draft PRC Data Security Law would primarily deal with data security, data governance and data trading,

with a focus on data other than personal information.

Other personal information protection rules

Apart from the previous three basic laws, personal information protection rules can be found in many different laws and regulations in China. Examples include the following laws of general application:

- Civil Code of the PRC (PRC Civil Code);
- Criminal Code of the PRC (PRC Criminal Code);
- Law of the PRC on the Protection of Rights and Interests of Consumers (PRC Consumer Protection Law)
- Provisions on Network Protection of Personal Information of Children
- Methods for Identifying Unlawful Acts of Collection and Use of Personal Information via Mobile Applications (regulating the processing of personal information via mobile applications)
- Interpretations of the Supreme People's Court and the Supreme Procuratorate on Several Issues Concerning Handling of Cases Involving Infringement upon Personal Information of Citizens

In addition, various authorities have formulated national standards and guidelines to establish recommended practices that businesses should follow when processing personal information in China. One of the most important standards is the Information Security Technology — Personal Information Security Specification (PRC Personal Information Security Specification), last amended on 6th March, 2020.[7] While these standards and guidelines are not mandatory in nature, Chinese regulators would likely refer to them when assessing an organisation's compliance with personal information protection requirements. There are also industry-specific and sector-specific regulations and standards in China that impose more detailed or stricter requirements in particular lines of business, especially more heavily regulated industries such as financial services (including banking, securities and insurance), healthcare and telecommunications, which are not addressed herein for the sake of length.

In this regard, China is not dissimilar from the United States, the prevalent practice of which is also to have numerous and varying data protection rules across a range of laws, regulations and other legal instruments at various levels of government. In the EU, most data protection rules are in the GDPR and at the EU level.

PERSONAL INFORMATION PROTECTION AUTHORITIES IN THE PRC AND THEIR POWERS

A handful of authorities in the PRC currently have the power to enforce compliance with laws against private companies and individuals. Thus far, the Cyberspace Administration of China (CAC) has taken the lead in formulating the implementation rules and measures of the basic laws. It is anticipated under the Draft PRC Personal Information Protection Law that the CAC will be the authority in charge of the overall planning and coordination of the protection of personal information and relevant regulatory affairs.[8] Aside from the CAC, industrial regulators are and will continue to be responsible for overseeing and enforcing various personal information protection requirements within their respective purview. Such regulators include, for example, the Ministry of Public Security (ie the major regulator supervising network security) or its local public security bureau (PSB), the Ministry of Industry and Information Technology (ie the major regulator of the telecommunications sector in China), the State Administration for Market Regulation (ie the general market regulator in China looking after consumers' rights and welfare) and the People's Bank of China (ie the central bank and main

regulator of the finance sector in China). When referring to 'personal information protection authority(ies)' in China, this paper refers to the CAC and, to the extent applicable, industrial regulators at national, provincial and municipal levels.[9]

Under EU data protection laws, the member states of the EEA have to establish supervisory authorities that must be independent from the general government administration and exercise supervision over private sector companies and also over law enforcement and other state agencies. When individual member states of the EU failed to comply with the independence requirements, the European Commission compelled changes in national law to ensure that national governments cannot influence the data protection authorities.[10] By contrast, the United States has tasked courts and general law enforcement authorities, the Federal Trade Commission, the Department of Health and Human Services and various other regulators and institutions to enforce privacy laws. California is establishing the first specialised Privacy Protection Agency in the United States pursuant to a popular ballot initiative that the California voters accepted at the 2020 general election,[11] but other states have not yet followed suit and the focus of the California Privacy Protection Agency will be limited to private sector activities within California's jurisdiction.[12]

The PRC is unlikely to adopt the EU model of independent data protection watchdogs as a check and balance also against EU and national authorities. As in the EU and United States, personal information protection authorities in China issue policies, administrative regulations and guidance regarding their respective jurisdiction and are administrative agencies rather than judiciary authorities.

Under the laws and regulations currently in effect in China, personal information protection authorities have the power to investigate violations and compel rectifications, and organisations and individuals must cooperate with such orders where they are based on legitimate grounds. The Draft PRC Personal Information Protection Law also provides details regarding personal information protection authorities' powers, including to provide personal information protection education to the public; handle complaints and reports related to illegal personal information processing activities; make inquiries of concerned persons; examine contracts, records and other relevant documentation; conduct on-site investigations; inspect and seize equipment and goods that evidence shows to have been used in illegal personal information processing activities; interview responsible personnel in a personal information breach and take steps to impose the types of sanctions discussed in the section on sanctions and penalties near the end of this paper.[13] These powers are similar in breadth to those vested in EU and US authorities with respect to private sector activity.[14]

SCOPE OF THE PRC PERSONAL INFORMATION PROTECTION RULES

Who and what personal information is protected by Chinese Personal Information Protection laws?

The Chinese Personal Information Protection Laws, which are of territorial jurisdiction, protect the personal information of Chinese residents.

By contrast, the GDPR protects the personal data of any individual — regardless of their immigration status or location — as long as the processing of such personal data is subject to the GDPR. Thus, companies established in the European Economic Area (EEA) must process individuals' personal data in accordance with the GDPR regardless of the location or immigration status of the data subject, and companies established outside the EEA that are subject to the GDPR must process the personal data of individuals located in the EEA in accordance with the regulation.[15]

Some US privacy laws specify that they only apply to residents of their respective jurisdiction, such as the CCPA and VCDPA. Other US privacy laws are silent on the topic and can be interpreted to protect persons who are in the United States.[16]

The PRC Cybersecurity Law, PRC Civil Code and Draft PRC Personal Information Protection Law define 'personal information' consistently as 'all kinds of information, whether recorded in electronic or other formats, that can be used to independently or in combination with other information to identify an individual'.[17] This definition is similar to the GDPR, which defines personal data to mean any information relating to an identified or identifiable natural person and does not define the term in relation to any particular format. Some US privacy laws are broader and some are narrower. For example, the CCPA defines 'personal information' to include information about households,[18] whereas the Security Rule of HIPAA only governs electronic information and California's breach notification law only covers computerised data.[19]

The Draft PRC Personal Information Protection Law defines 'sensitive personal information' as 'personal information that, if leaked or illegally used, could lead to discrimination against individuals or serious harm to personal or property safety'. Examples given in the law include race, ethnicity, religious beliefs, personal biometrics information, medical health information, financial account information and personal whereabouts.[20] The GDPR, CCPA, VCDPA and other US laws take a different approach by defining the subset of personal information that must be handled more sensitively in an exhaustive manner. For instance, the GDPR establishes more onerous processing requirements with respect only to certain special categories of personal data and data relating to criminal convictions and offenses.[21] Similarly, the CCPA and VCDPA define 'sensitive personal information' and 'sensitive data' respectively to include only certain categories of personal information.[22] There are differences among the lists of sensitive personal information under all of the laws—for example, unlike the CCPA and the Chinese law, the GDPR does not subject processing of financial account information to special requirements.

Who must comply with Chinese personal information protection laws?

The PRC Cybersecurity Law's rules on the processing of personal information generally apply to all sectors and types of organizations with no specific exemptions. The Draft PRC Personal Information Protection Law would apply to all sectors, all types of organizations (including government agencies[23]) and all processing activities except for (i) processing of personal information by PRC government agencies when carrying out statistical or file management activities, which may be governed by special rules,[24] and (ii) the processing of personal information by an individual for personal or family reasons.[25]

The proposed scope of the Draft PRC Personal Information Protection Law is similar in comprehensiveness to the GDPR's material scope, which generally covers all industries including the private and public sectors, subject to exemptions for processing by individuals during personal and household activities and certain public bodies.[26] The United States does not have a similarly comprehensive privacy statute. Even the CCPA and VCDPA have significant carve-outs such as for entities covered by HIPAA, and VCDPA only applies to individuals acting in an individual or household context and not in a commercial or employment context.[27]

What types of processing do the PRC personal information protection rules cover?

The PRC Civil Code and Draft PRC Personal Information Protection Law

define 'processing' as 'collection, storage, use, processing, transmission, provision, disclosure and other activities of personal information'.[28] Thus, the PRC personal information protection rules cover all types of processing throughout the lifecycle of personal information. This is similar to and possibly even broader than the GDPR. The GDPR defines 'processing' broadly as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means'.[29] But the GDPR does not apply to processing that does not involve any automated means and where the personal data is not intended to form part of a filing system.[30] The CCPA and VCDPA's definitions of 'processing' mirror the core definition found in the GDPR.[31]

Do the PRC personal information protection rules apply extra-territorially to organizations or individuals outside of the country?

Traditionally, Chinese personal information protection rules and the personal information protection authorities have focused on individuals, organizations and activities within the PRC territory and refrained from trying to regulate or enforce laws against persons or organizations acting outside of the PRC territory.[32] The PRC Cybersecurity Law and other laws and regulations currently in effect are generally not applicable to foreign organizations operating outside of the PRC.

However, China now seems to be expanding the geographic focus of its personal information protection regime in the Draft PRC Personal Information Protection Law. In particular, the Draft PRC Personal Information Protection Law contemplates that it applies to processing activities conducted outside of the PRC involving personal information of Chinese residents where the processing activities: (i) are for the purpose of offering products or services to individuals in China; (ii) relate to analysis of the behavior of individuals in China; or (iii) meet other circumstances provided under the laws or administrative regulations.[33] Circumstances (i) and (ii) above closely parallel the circumstances in which the GDPR provides that it has extra-territorial effect.[34]

It is also worth noting that the Draft PRC Data Security Law contemplates that organizations and individuals located outside of the PRC could be penalized in accordance with Chinese law if their data processing activities jeopardize Chinese national security or public interests, or the legitimate rights and interests of the PRC citizens.[35]

These provisions of the Draft PRC Personal Information Protection Law and Draft PRC Data Security Law signal that the Chinese government is looking to strengthen the protection of personal information of Chinese residents against foreign organizations and individuals. It is highly likely that the principles of extra-territoriality discussed above will be retained in the final versions of these laws.

Do PRC laws recognise a right to privacy in addition to and separate from the right to personal information?

Yes. Rights pertaining to personal information and privacy are distinguished and protected by separate rules under Chinese laws. The PRC Civil Code establishes a general right to privacy, similar to US tort law and national laws in the EU.[36] The law defines 'privacy' as the 'private life of individuals which is not to be intruded, as well as private space, private activities and private information of individuals that they do not desire others to know about'.[37] The PRC Civil Code establishes that the following constitute violations of one's right to privacy unless there is a lawful basis to do so or the right holders have provided their express consent:

(i) intruding on the private life of others by means of phone calls, text messages,

instant message tools, emails, leaflets or the like;
(ii) entering, photographing or spying on any private space such as residence or hotel room;
(iii) filming, spying on, eavesdropping or disclosing the private activities of others;
(iv) photographing or spying on the private body parts of others;
(v) processing the private information of others; and
(vi) intruding on the right of privacy of others through other means.

The PRC Civil Code is of territorial jurisdiction[38] but not personal jurisdiction. Accordingly, the above rules associated with the right to privacy apply to the juristic acts that occur within the PRC territory. The Draft PRC Personal Information Protection Law and the other requirements discussed in this paper establish an individual's right of personal information. The EU and United States do not distinguish conceptually between rights of privacy and personal information—in general, the unauthorised or illegal processing of an individual's personal information are viewed as invasions of their privacy in these jurisdictions.

CONTROLLER VS. PROCESSOR: IN WHAT WAYS DO CHINESE PERSONAL INFORMATION PROTECTION LAWS DISTINGUISH BETWEEN CONTROLLERS AND PROCESSORS?

China currently does not statutorily distinguish between controllers and processors, but the Draft PRC Personal Information Protection Law would create such a distinction, in line with the GDPR and some US privacy laws.[39]

Under the PRC Cybersecurity Law and other Chinese laws and regulations currently in effect, all businesses, regardless of their role in the processing of personal information (*i.e.*, whether they act in practice as a controller or processor), are similarly regulated. However, the Draft PRC Personal Information Protection Law adopts a concept similar to the controller promulgated in the GDPR and some US privacy laws and defines it as 'an organization or individual that may independently determine the purposes and means, etc. of the processing of personal information'.[40] However, the draft law uses the term 'personal information processor' to refer to this type of entity. To avoid confusion, this paper refers to this type of entity as a 'controller'. The Draft PRC Personal Information Protection Law also establishes a concept similar to joint controllers under the GDPR.[41] Controllers are subject to virtually all personal information protection requirements under the law.

The Draft PRC Personal Information Protection Law does not establish a definition for 'processor' but provides that a controller may entrust another person to process personal information on its behalf with the controller still responsible for compliance with the majority of personal information processing obligations.

CONTROLLER RESPONSIBILITIES

Do the principles of accuracy, purpose limitation, and retention limitation apply in China?

Yes, to some extent. The PRC Cybersecurity Law, Draft PRC Personal Information Protection Law and other laws and regulations in China generally provide that personal information must be up-to-date, accurate and complete for the purposes of processing; otherwise, individuals may request that their personal information be updated, supplemented or rectified.[42] The GDPR establishes a similar principle that personal data shall be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to

the purposes for which they are processed, are erased or rectified without delay'.[43] US privacy laws generally do not establish a similar affirmative principle, although some US privacy laws including HIPAA, the CCPA and VCDPA give or will give individuals the right to correct inaccurate personal information held by a controller.[44]

In addition, PRC laws recognise the principle of purpose limitation whereby a controller must collect or process personal information only where relevant to and necessary for the intended purposes of processing.[45] This principle is articulated variously in the GDPR and a number of US privacy laws, including HIPAA, the CCPA and VCDPA.[46] In addition, if a controller would like to process personal information for additional or different purposes, it may only proceed with the personal information subject's fresh consent. The GDPR and VCDPA similarly restrict controllers from processing personal data for additional purposes without a lawful basis.[47] Under the CCPA, the controller is arguably only required to notify, and not necessarily obtain consent from, the data subject before processing personal data for additional purposes.[48]

Regarding the retention of personal information, the Draft PRC Personal Information Protection Law would codify a rule currently found in the PRC Personal Information Security Specification by requiring organizations to retain personal information for the minimum period necessary to achieve the purposes of processing.[49] This aligns with requirements under the GDPR and, starting in 2023, the CCPA, and VCDPA.[50]

Will foreign controllers have to establish a local representative in China?

Yes. The Draft PRC Personal Information Protection Law provides that a controller that is domiciled outside of the PRC but processes personal information of Chinese residents must establish a dedicated local organization or representative in China, similar to the requirement in Article 27 of the GDPR except that the requirement only applies to controllers.[51] In the United States, companies (whether controller or processors) have to register with secretaries of state to do business within a state, and appoint a representative for service of process, but foreign companies are not required to separately appoint an authorised representative for purposes of compliance with data privacy laws.[52]

Under the Draft PRC Personal Information Protection Law, the local organization or representative would be responsible for handling the relevant affairs concerning the protection of personal information of Chinese residents and the foreign controller must report the local organization or representative's name and contact details to the PRC personal information protection authorities.[53] By contrast, the GDPR only requires that the representative's contact details be included in privacy notices. It remains to be clarified whether the local organization or representative might be penalized merely as a result of a foreign controller contravening Chinese personal information protection requirements, but the authors take the view that such likelihood would be low. In the EU, this depends on national laws; for example, in Spain, a local representative may be liable for the foreign entity's violations whereas this is not the case in other member states.

On what lawful grounds may controllers process personal information?

Under the PRC Cybersecurity Law and other Chinese laws and regulations currently in effect, the sole legal grounds for the processing of personal information is the data subject's consent. Typically, a general consent to an organization's overall personal information processing activities (including

the processing of sensitive personal information and outbound transfers of personal information) is sufficient.

However, the Draft PRC Personal Information Protection Law would supersede the current consent-based regime, and establish both consent and non-consent-based legal bases for the processing of personal information. Under the law, a controller would be permitted to process personal information *only if:*

- Informed consent from the personal information subject has been obtained;
- It is necessary for the controller to enter into or perform a contract to which the personal information subject is a party;
- It is necessary for the controller to perform a statutory duty or legal obligation;
- It is necessary for the controller to respond to an unexpected public health incident or, in an emergency, to protect the life, health or property of individuals;
- It is in the public interest for the purposes such as monitoring news reports and public opinion, and to the extent that such processing is reasonable; or
- It falls within other circumstances provided by laws and administrative regulations.[54]

These legal bases of processing resemble those enumerated under Article 6(1) of the GDPR except that the GDPR also includes the pursuit of legitimate interests, which controllers in the EU rely on in many circumstances, whereas the Draft PRC Personal Information Protection Law does not. Unlike the GDPR and Draft PRC Personal Information Protection Law, the CCPA and VCDPA do not generally prohibit the processing of personal information unless certain legal grounds apply. But these state laws do require consent in certain circumstances. For example, the CCPA requires businesses to obtain consent to sell certain minors' personal information, and the VCDPA requires businesses to obtain consent to process Virginia residents' sensitive personal information.[55]

What information will controllers have to include in their privacy notices?

Under the Draft PRC Personal Information Protection Law, controllers will generally have to provide the following details to individuals before collecting their personal information and before individuals are able to give their legally effective and binding consent:

- The identity and contact details of the controller;
- The purposes and means of processing;
- The scope of personal information to be processed;
- The period for which personal information will be stored;
- A description of individuals' rights pertaining to their personal information under the law and the ways and procedures in which they can exercise their rights; and
- Any other information required by laws and administrative regulations.[56]

Additional details must be included if the controller will process sensitive personal information or transfer personal information to another person located within or outside of China (see Section 5.7 below). The Draft PRC Personal Information Protection Law would require controllers to furnish these details whether the controller collects personal information directly from individuals or from another source.

By way of comparison, the GDPR, CCPA and VCDPA require controllers and businesses to include some of these details, and other details, in their privacy notices. For example, the GDPR also requires controllers to identify the lawful basis used to justify the processing, and information about the source of the personal data if it was collected from a source other than the data subject.[57] The CCPA and VCDPA also require or will

require businesses to explain whether they sell personal information or share it for cross-context behavioral or targeted advertising purposes.[58] Many companies deal with these disparate informational requirements by preparing separate or supplemental privacy notices addressed to individuals in different geographical regions. Depending on what other details the finalised Chinese laws will require controllers to include in their privacy notices, this may be necessary for China as well.

What rights may Chinese data subjects exercise?

Under the PRC Cybersecurity Law and Chinese laws and regulations currently in effect, data subjects have the right to access and make a copy of their personal information, and request that their personal information be updated or deleted.[59] The Draft PRC Personal Information Protection Law would give individuals a broader suite of rights with respect to their personal information. In particular, the law would permit individuals to:

- Know about and decide on the processing of their personal information, including to restrict or refuse the processing of their personal information, unless otherwise provide by laws and administrative regulations;
- Access and make copies of their personal information, unless the processing is required by law to be kept confidential or notification is otherwise not required;
- Request that a controller update or supplement their personal information if it is inaccurate or incomplete;
- Request that their personal information be deleted where:
  - the agreed retention period has expired or the purposes of processing have been achieved;
  - the controller has ceased to offer the products or services;
  - individuals have withdrawn their consent and the processing is based on their consent;
  - the controller has processed personal information in violation of law or in breach of their agreement with individuals; or
  - other circumstances provided by laws or administrative regulations apply; and
- Request that a controller provide an explanation of the rules governing the processing of their personal information.[60]

Notably, the Draft PRC Personal Information Protection Law would not give individuals the right to access copies of their personal information that a controller holds about them in a portable manner, as the GDPR, CCPA and VCDPA do or will do.[61]

The Draft PRC Personal Information Protection Law also proposes that any organization or individual shall have the right to lodge a complaint with or report to a competent personal information protection authority in respect of an illegal personal information processing activity. The authority must handle the case and inform the person who lodged the report of the outcome.[62] This type of mechanism resembles the reporting mechanisms used in the EU and United States.[63]

In what circumstances is consent required and when is it valid?

Consent is one of the legal bases for the processing of personal information under the Draft PRC Personal Information Protection Law. Controllers will most likely rely on consent if the controller will not enter into a contract with the data subject, is not legally required to process personal information, and is not processing personal information in the context of an emergency or for public interests. If consent will be the legal basis of processing, the data subject must always give their informed consent prior to processing (*i.e.*, they must have received a

notice containing the details described in Section 5.4 above). However, there are two exceptions. First, a controller does not have to inform data subjects if the processing is required by law to be kept confidential or notification is otherwise not required (see, e.g., Section 10 on government surveillance below). Second, if, in order to protect the life, health or property of individuals in an emergency, the controller is not able to timely inform individuals of the processing of their personal information, the controller does not have to provide prior notice but must inform them thereof after the emergency is resolved.[64] Where data subjects are minors below the age of 14, consent form their legal guardian is required.[65]

Will the rules with respect to notification and consent requirements be more stringent for sensitive personal information and transfers of personal information?

Yes, the Draft PRC Personal Information Protection Law would impose stricter notification and consent requirements in the context of the processing of sensitive personal information and either domestic or international transfers of personal information.

With respect to notification requirements, a controller that seeks to process sensitive personal information would also have to inform data subjects specifically of (i) the necessity of processing and (ii) the impacts of the processing on them.[66] A controller that intends to transfer personal information to another person within the PRC shall additionally inform data subjects of (i) the corporate identity and contact details of the other person, (ii) the purposes and means of processing and transfer of personal information and (iii) the scope of personal information to be transferred.[67] A controller that wishes to transfer personal information across the Chinese border has to include the following additional details in its privacy notice: (i) the corporate identity and contact details of the foreign recipient of personal information (acting either as a controller or processor), (ii) the purposes and means of processing and cross-border transfer of personal information, (iii) the scope of personal information to be exported and (iv) the rights made available by the foreign recipient to the data subjects residing in China.[68] On the face of this rule, the identity and contact details of the foreign recipient should be disclosed to the data subjects and a general description on the types of the foreign recipient may not be sufficient. But, there are criticisms of this rule on the grounds that it may be too burdensome for the controller to identify and disclose each and every foreign recipient to data subjects and seek their valid consent. It remains to be seen how these rules will look in the final version of the law.

The GDPR imposes different disclosure requirements on controllers that engage in cross-border transfers of personal data. Under the GDPR, controllers have to inform data subjects, where applicable, that they intend to transfer personal data to a country outside of the EEA or an international organisation and the safeguards they have implemented or relied on to satisfy the GDPR's cross-border transfer requirements. Controllers also have to make copies of such safeguards available to data subjects on request. Unlike the Draft PRC Personal Information Protection Law, controllers do not have to identify each foreign recipient of a data subject's personal data, only the 'categories of recipients' of such data.[69] The United States generally does not require companies to make any additional disclosures if they intend on transferring an individual's personal information across borders.

The Draft PRC Personal Information Protection Law would require specific and separate prior informed consent from data subjects to (a) process their sensitive personal information and (b) transfer their personal information across borders.[70] In other words,

should the law be adopted as currently drafted, general consent would no longer be considered sufficient for the aforementioned activities. The GDPR does not categorically require companies to obtain a data subject's consent before transferring their personal data across borders, but the GDPR contemplates that explicit consent may legitimize such transfers if certain approved safeguards or mechanisms do not apply and the data subject has been sufficiently informed of relevant risks.[71] The United States generally does not require companies to obtain a data subject's consent to transfer their personal information across borders.

Are there data residency requirements in China?

Yes. The PRC Cybersecurity Law requires critical information infrastructure operators to store all personal information that they have collected and generated in the course of domestic operations within Chinese territory.[72] The PRC Cybersecurity Law defines 'critical information infrastructure' as 'infrastructure that, if destroyed, disabled, or suffering a data leak, would seriously endanger national security, national welfare, people's livelihood, or the public interest'.[73] Illustrative examples include public communication and information services, energy, transportation, water conservancy, finance, public service and e-governance affairs.[74] The exact scope of critical information infrastructure is not fully settled for the time being and expected to be further clarified by way of implementing measures.

The Draft PRC Personal Information Protection Law would add the following data residency requirements:

(i) Controllers (and not just critical information infrastructure operators) that process personal information above certain prescribed volumes must store in China the personal information that they collect and generate in the course of their domestic operations;[75] and
(ii) Government agencies must store personal information that they process in China.[76]

What other special rules apply to the transfer of personal information internationally?

Under the Draft PRC Personal Information Protection Law, if a controller wishes to export personal information that is collected or generated in connection with its Chinese business operations to a foreign recipient of personal information outside of the PRC, the personal information export activities must be for genuine business needs. Additional requirements may apply depending on the circumstances.

First, a controller will generally be required to undergo security assessments as a prerequisite to being permitted to transfer personal information outside of China if it (i) processes an aggregate volume of personal information that surpasses certain thresholds (the exact figures have not yet been currently defined), (ii) is an operator of critical information infrastructure or (iii) is a government agency. If a controller falls within category (i) or (ii) earlier, under the Draft PRC Personal Information Protection Law, it would have to obtain approval from the CAC after being subject to a security assessment to transfer personal information about Chinese residents outside of China.[77] If a controller is a government agency (ie category (iii)), under the law, it would need to conduct a security assessment, to which the relevant state departments may provide assistance and support, but no approval from the CAC would likely be necessary.[78] Further discussion of requirements regarding security assessments is provided in the section 'Under what circumstances must an entity perform a security assessment in China?' later in this paper.

Secondly, the controller may have to obtain a personal information protection

certification from an eligible institution in accordance with the CAC's regulations. Details of the circumstances triggering certification, the certification requirements and the scope of qualified certifying institutions are currently unclear and require further clarification. While the GDPR also provides for the establishment of data protection certification mechanisms, certifications would be voluntary and not required for cross-border transfers of personal data.[79]

Thirdly, the controller may have to enter into a legally compliant contract with the foreign recipient concerning the export of personal information. It is not entirely clear when and how this requirement will apply. But it is anticipated that this would be a default requirement that applies to all controllers who wish to transfer personal information collected or generated in China or outside of China.[80]

The US private sector privacy laws generally have no analogous requirements with respect to cross-border transfers of personal information.

In what circumstances is the appointment of a data protection officer (DPO) required?

Under the Draft PRC Personal Information Protection Law, controllers that process an aggregate volume of personal information that surpasses certain thresholds (the exact figures have not yet been currently defined) have to designate a data protection officer (DPO). Also, all critical information infrastructure operators will have to designate a DPO.[81] The DPO position under the draft Chinese law is similar in scope to the DPO position under the GDPR. The GDPR also requires entities to designate a DPO only if it meets certain conditions, such as processing special categories of personal information 'on a large scale'.[82] The United States generally does not require companies to appoint a DPO, but HIPAA is an exception. This law requires covered entities to appoint privacy and security officials responsible for implementing required privacy and security measures. Business associates also have to appoint a security official but not a privacy official.[83]

What requirements apply to electronic marketing in China?

Electronic marketing is generally only permissible in China with the consent or on the request of recipients. The relevant laws are the PRC Consumer Protection Law,[84] the Advertising Law of the PRC, the Administrative Rules for Internet E-mail Services (E-mail Rules) and the Administrative Rules for Communication Short Message (SMS) Services (SMS Rules), which do not establish any exceptions to the requirement to obtain consent. Specifically, according to the E-mail Rules[85] and SMS Rules,[86] the distribution of commercial advertisements via e-mail and SMS would not be legitimate and compliant unless recipients give their opt-in (express) consent. That said, making commercial calls and distributing commercial advertisement materials to individuals' residence by postal e-mail is generally acceptable on an opt-out basis under the current legal regime. Further, an easily accessible opt-out mechanism must be made available to recipients.[87] The Draft PRC Personal Information Protection Law proposes that controllers will be required to provide individuals with an option that marketing messages sent by automated decision-making[88] are not based on user profiles.[89]

These regimes vary from those in the EU and United States. The EU also generally requires prior opt-in consent to send electronic marketing messages to individuals, although there are exceptions such as to market similar products to prior customers who had an opportunity to opt-out.[90] The United States generally establishes an opt-out regime for marketing e-mails but an opt-in regime for marketing text messages.[91]

PROCESSOR RESPONSIBILITIES: WHAT OBLIGATIONS DOES THE PRC LAW IMPOSE ON PROCESSORS?

The Draft PRC Personal Information Protection Law would impose the following requirements on a person who processes personal information on behalf of a controller:

(i) To process personal information according to the purposes and means of processing agreed with the controller;
(ii) Not to process personal information for any other purpose or using any other means beyond the scope of agreement with the controller;
(iii) Return personal information to the controller or delete personal information after completion of performance of contract; and
(iv) Unless the controller consents, not to further entrust a third party to process personal information.[92]

These rules mirror some, but not all, of the key obligations that apply to processors or their equivalents under the GDPR, CCPA and VCDPA. For example, the GDPR does, and the CCPA and VCDPA will, require processors to assist controllers in responding to requests from data subjects to exercise their privacy rights.[93] At the same time, the CCPA and VCDPA do not expressly require processors to obtain the controller's consent to disclose personal data to downstream processors, like the GDPR does[94] and the Draft PRC Personal Information Protection Law would.

DATA SECURITY

What data security requirements apply under Chinese law?

Chinese laws currently impose general data security requirements that apply to networks and personal information, and the Draft PRC Personal Information Protection Law would introduce more specific security requirements that apply to personal information.

The PRC Cybersecurity Law and its implementation rules and guidelines impose requirements on network operators, including compliance with the law's so-called multilevel network security protection scheme.[95] The PRC Cybersecurity Law also obliges network operators generally to adopt technical and other necessary measures to ensure the security of personal information, take steps to avoid its leakage, destruction or loss, and immediately take remedial actions if a personal information security incident has occurred or is likely to occur.[96]

The Draft PRC Personal Information Protection Law would introduce more detailed data security obligations that apply to personal information. Under the law, a controller must, based on the purposes and means of processing, types of personal information processed, impacts on personal information subjects and potential security risks to be entailed, adopt the following data security measures:

- Formulate an internal management system and operating rules;
- Administer personal information according to different grades and categories;
- Implement corresponding security technical measures such as encryption and de-identification;
- Set reasonable limits for the authority of operators to process personal information and regularly conduct security education and training for employees;
- Formulate and organise the implementation of a contingency plan for personal information security incidents; and
- Implement other measures prescribed by laws and administrative regulations.[97]

A controller must also regularly review and evaluate the compliance status of the personal information processing activities and the implemented protective measures.[98]

The GDPR takes a similar approach to data security, requiring controllers and processors to take into account various considerations such as the nature of processing and the costs of implementation, and accordingly implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The GDPR lists some examples of safeguards that may be appropriate, including the pseudonymisation and encryption of personal data, incident response protocols and a process for regularly testing, assessing and evaluating the effectiveness of security measures.[99]

The United States varies in its approach to data security. Some US laws impose very specific data security requirements with respect to particular types of products. For example, California requires manufacturers of devices that can connect to the internet to ensure that such devices require their user to generate a new means of authentication before access is granted to the device for the first time.[100] As another example, HIPAA imposes detailed security requirements on covered entities and business associates, from 'procedures to create and maintain retrievable exact copies of electronic protected health information' to 'procedures for removal of electronic protected health information from electronic media before the media are made available for re-use'.[101] At the same time, some US laws take a more general approach to data security. For example, a California statute generally requires a 'business that owns, licenses, or maintains personal information about a California resident [to] implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorised access, destruction, use, modification, or disclosure'.[102] The statute does not prescribe specific safeguards that have to be implemented to address this duty.

Under what circumstances must an entity perform a security assessment in China?

The Draft PRC Personal Information Protection Law would require a controller to conduct a security assessment before carrying out any of the following processing activities:

- Process sensitive personal information;
- Use personal information for automated decision-making;
- Entrust a processor to process personal information;
- Provide personal information to a third party or make personal information public;
- Provide personal information to a foreign recipient out of the PRC; or
- Engage in other processing activities that have a material effect on the personal information subjects.[103]

The security assessment must analyse (i) whether the purposes, means and other aspects of processing are lawful, proper and necessary; (ii) the extent of the impacts on, and risk for, the personal information subjects and (iii) whether the adopted protective measures are lawful, effective and commensurate with the degree of risk involved. Records of security assessments would need to be retained and archived for at least three years.[104] A national standard with recommended effect ¾ ie Information Security Technology — Guidance for Personal Information Security Impact Assessment[105] ¾ has been formulated to provide guidance on the principles and process flows of security assessment in this conjuncture.

As mentioned in the section 'What other special rules apply to the transfer of personal information internationally?' earlier in this paper, cross-border transfers of personal information trigger security assessment requirements for controllers that process certain volumes of personal information, critical information infrastructure operators and government agencies. In these instances,

the draft Measures for Security Assessment of Export of Personal Information (Draft PRC Security Assessment Measures), published by the CAC on 13th June, 2019, for public comment shed some light on the intended regulatory scheme.[106] The Draft PRC Security Assessment Measures contemplates that, prior to the export of any personal information, an exporter of personal information must:[107]

(i) Conduct a self-assessment of security risks associated with the intended export and the security safeguards and measures to be adopted to address such risks;
(ii) Prepare a security assessment report;
(iii) File the report with the provincial counterpart of the CAC for its review; and
(iv) Obtain clearance from the CAC.

The Draft PRC Security Assessment Measures also propose that (a) the security assessment would need to be conducted separately in respect of export of personal information to each foreign recipient; and (b) multiple transfers or continuous transfer of personal information to the same foreign recipient would not trigger separate security assessment, provided that a new security assessment would still be required (x) once every two years or (y) where there is any change in (A) the purpose of export of personal information, (B) the types of exported personal information or (C) the retention period by the same foreign recipient during the ongoing export of the relevant personal information.[108] Further, certain ongoing compliance requirements are included under the draft measures, for example, (i) exporters would be required to establish and maintain records of exporting personal information for five years covering the certain aspects of transferred personal information; and (ii) exporters would have to submit an annual report on its export of personal information within the relevant calendar year to the provincial counterpart of the CAC by 31st December of each calendar year.[109]

The Draft PRC Personal Information Protection Law requirements outlining specific security measures to be implemented vary from those under the GDPR in that they only apply to controllers[110] — however, the requirements under the PRC Cybersecurity Law and other rules apply to all network operators and therefore would also apply to processors. The circumstances in which an assessment is required under the Draft PRC Personal Information Protection Law are more extensive than those prescribed by the GDPR. The GDPR requires a controller to conduct a data protection impact assessment where the planned processing operations are 'likely to result in a high risk to the rights and freedoms of natural persons'.[111] The conditions under the Draft PRC Personal Information Protection Law extend beyond where such risks exist and are triggered based on potentially routine processing activities such as relying on a processor. Some US laws require security assessments in certain circumstances including the Security Rule of HIPAA and the VCDPA, and in those laws, the specifics are also different.[112] Neither the GDPR nor US private sector privacy laws require personal information security assessments to be reviewed and approved by regulators.

Does Chinese law impose obligations to notify authorities or individuals in case of a personal information breach?

Chinese laws currently establish breach notification requirements, but enforcement of these obligations has not been very strict.[113]

The Draft PRC Personal Information Protection Law prescribes more specific breach notification requirements, although it is still currently unclear what authority would be responsible for receiving such

notifications. Under the law, a controller that discovers the leakage (ie a breach) of personal information must immediately take remedial steps and notify the personal information protection authority and affected personal information subjects of certain details. These include:[114]

- The cause of personal information leakage;
- The types of personal information leaked and the harm that may be entailed;
- The remedial actions that have been taken;
- The actions that the personal information subjects may take to mitigate the harm; and
- The contact details of the controller.

Like the GDPR, a breach involving any categories of personal information may trigger breach notification obligations. By contrast, US breach notification obligations are only triggered where certain prescribed categories of personal information, such as Social Security Numbers and payment card details, are subject to unauthorised access or acquisition.[115]

In addition, the Draft PRC Personal Information Protection Law does not establish thresholds whereby breach notifications to the personal information protection authority are required only if certain conditions are met, such as if risks of harm or the number of affected personal information subjects surpass certain levels. However, the Draft PRC Personal Information Protection Law provides that, if the controller has adopted measures that can effectively prevent the data leakage from causing harm, it may opt not to notify affected personal information subjects, unless the personal information protection authority disagrees and instructs the controller to notify such individuals.[116] Some interpret this as a signal that the Chinese government will more actively enforce breach notification requirements in the near future.

The Draft PRC Personal Information Protection Law's lack of thresholds for notifying personal information protection authorities would likely result in a higher volume of breach notifications in China versus the EU and United States. The GDPR only requires notifications to authorities where risks to individuals' rights and freedoms are not unlikely.[117] Only a subset of US states require breach notifications to government agencies, and a number of these only require such notifications where more than a certain number of data subjects were affected.[118]

RECORD-KEEPING: WHAT TYPES OF RECORDS MUST ENTITIES KEEP UNDER CHINESE PERSONAL INFORMATION PROTECTION LAWS?

The PRC Cybersecurity Law, Draft PRC Personal Information Protection Law and other generally applicable laws and regulations in China do not prescribe a list of information, records or documents to be retained in relation to the processing of personal information. Unlike the GDPR, the Draft PRC Personal Information Protection Law would not require organisations to maintain a comprehensive record of processing activities, although such a requirement may be included in future versions of the law or its implementation rules. But the Draft PRC Personal Information Protection Law and other Chinese laws prescribe retention requirements with respect to specific types of records — for example, the Draft PRC Personal Information Protection Law requires controllers to maintain records of security assessments for at least three years.[119] The US privacy laws also generally do not require companies to maintain comprehensive records of processing activities but do establish retention requirements with respect to specific types of records. For instance, HIPAA requires entities subject to the law

to retain compliance policies and procedures and certain security-related documents to be retained for at least six years,[120] and the CCPA requires records of responses to data subject requests to be retained for at least two years.[121]

REGISTRATIONS WITH AUTHORITIES: ARE THERE ANY REQUIREMENTS TO REGISTER PERSONAL INFORMATION PROCESSING WITH THE PRC PERSONAL INFORMATION PROTECTION AUTHORITIES?

The Draft PRC Personal Information Protection Law would require foreign controllers of Chinese residents' personal information to establish a dedicated organisation or designate a representative in China and submit the domestic organisation or representative's name and contact details to the personal information protection authority (see the section earlier in this paper 'Will foreign controllers have to establish a local representative in China?'). The Draft PRC Personal Information Protection Law would also require controllers that wish to transfer certain volumes of Chinese residents' personal information outside of China to undergo a security assessment administered by the CAC (see the section 'Under what circumstances must an entity perform a security assessment in China?' earlier in this paper) and obtain the CAC's clearance (see the section 'What other special rules apply to the transfer of personal information internationally?' earlier in this paper). Otherwise, the PRC Cybersecurity Law, Draft PRC Personal Information Protection Law and other generally applicable laws and regulations in China do not require organisations to register the processing of personal information with local personal information protection authorities.

Prior to the implementation of the GDPR, EU member states required organisations to notify, register with or obtain approvals from local personal information protection authorities in certain circumstances. The GDPR generally did away with such requirements.[122] As mentioned earlier, however, the GDPR does require foreign entities subject to the regulation to designate a local representative. The GDPR also requires controllers to notify local supervisory authorities of the contact details of their DPOs,[123] but there is no analogous requirement with respect to local representatives' contact details. The United States generally does not require organisations to register with government agencies to process local residents' personal information, subject to some narrow exceptions such as the requirement that certain data brokers register with local authorities in California and Vermont.[124]

GOVERNMENT SURVEILLANCE: IN WHAT CIRCUMSTANCES MAY CHINESE AUTHORITIES INTERCEPT PRIVATE COMMUNICATIONS AND TAKE OTHER INVESTIGATIVE MEASURES?

Various laws authorise Chinese authorities to engage in the interception of communications, monitor and surveil individuals and take other investigative measures where there is a need to do so to investigate allegations of serious criminal offences and after proper approval has been obtained in accordance with statutory procedures.[125] Examples of such laws include the National Intelligence Law of the PRC, the State Security Law of the PRC, the Anti-Terrorism Law of the PRC, the Criminal Procedure Law of the PRC and the Supervision Law of the PRC. Examples of authorities that hold such powers include the national security administration, the PSB (when exercising its investigative powers), the people's procuratorate and certain other supervision authorities. Examples of serious criminal offences that may be investigated in this manner include crimes endangering national security, terrorist activities, crimes

of a triad nature, major drug-related crimes and major job-related crimes of civil servants (such as corruption and bribery). In these types of scenarios, the personal information subjects being investigated would generally not be informed and have limited rights to privacy or rights to personal information. The GDPR and US privacy laws also generally include exceptions to privacy protections where authorities investigate a party for wrongdoing[126] with privacy considerations also interlaced into criminal laws.[127]

SANCTIONS AND PENALTIES: WHAT SANCTIONS AND PENALTIES MAY APPLY FOR CONTRAVENING THE PRC PERSONAL INFORMATION PROTECTION LAWS?

Contravening the PRC personal information protection laws may result in regulatory and administrative fines, civil liability and criminal liability.

Under the PRC Cybersecurity Law, network operators that fail to protect personal information will be subject to a warning, confiscation of illegal gains, a fine of not less than one but not more than ten times the illegal gains (or if there is no illegal gain, a fine of up to RMB 1 million) or a combination of these administrative penalties. The infringement will be recorded in the credit files of the infringing network operator, which are publicly accessible. Any person directly in charge or responsible for the network operator may be subject to a fine of not less than RMB 10,000 but not more than RMB 100,000.[128]

Like the GDPR, the Draft PRC Personal Information Protection Law would establish fines for serious breaches that are measured in proportion to the yearly turnover of the institutional offender. For a severe violation of the law or in the absence of required data security measures, the personal information protection authority may impose a fine of the greater of (i) RMB 50 million (the analogous maximum under the GDPR is EUR 20 million); and (ii) 5 per cent of the offending entity's annual turnover in the preceding year (the analogous maximum under the GDPR is 4 per cent of global annual turnover). It is unclear whether the reference to annual turnover in the Draft PRC Personal Information Protection Law refers to worldwide turnover or domestic turnover generated from the Chinese market. This is expected to be clarified in the final version of the law or its implementation rules. The leading officer directly in charge or other directly responsible persons may be subject to a fine of up to RMB 1 million.[129] Additional penalties may apply on top of the aforementioned fines if warranted. The US privacy laws generally do not measure maximum fines as a function of an offending entity's revenue but can set high maximum amounts of fines on a per violation basis. For example, the Federal Trade Commission may impose fines of up to US$40,000 per violation of the Federal Trade Commission Act, which encompasses certain privacy-related infringements.[130]

The PRC Consumer Protection Law provides for civil remedies available to consumers (defined as those who purchase products or services for daily household consumption) whose personal information has been infringed upon by business operators, including the relevant business operators being ordered to cease the infringement, rehabilitate the consumer's reputation, take action to mitigate adverse consequences, provide an apology and/or provide indemnities. In addition, administrative authorities may impose monetary penalties of up to ten times the illegal income derived from an infringement or, if there is no illegal income, a fine of up to RMB 500,000 or/plus an order to suspend business for rectification or revoke the business license.[131]

Under the PRC Criminal Code, a penetrator who illegally sells or otherwise

illegally provides personal information to third parties may be subject to a fixed-term imprisonment of not more than three years or criminal detention (or in a severe case, a fixed-term imprisonment of not less than three years but not more than seven years) and, concurrently or separately, sentenced to a penalty. Where the penetrator is an entity, it would be sentenced to a penalty, while the directly responsible persons would be subject to imprisonment or criminal detention in accordance with the foregoing.[132]

Various data protection and privacy laws in the EU and United States also establish potential civil and criminal sanctions for violations,[133] reflecting the broad international consensus that a variety of enforcement tools are required to deter, penalize and remedy privacy violations.

References

1. Determann, L. and Gupta, C. (2019)' Indian Personal Data Protection Act of 2018: draft bill and its history, compared to GDPR and California Privacy Law', *Berkeley Journal of International Law*, Vol 37, p. 481.
2. Cal. Civ. Code § 1798.100 – 1798.199.100.
3. Senate Bill No. 1392, available at: https://lis.virginia.gov/cgi-bin/legp604.exe?211+ful+SB1392ES1 (accessed 3rd May, 2021). The VCDPA becomes effective on January 1, 2023.
4. See, e.g., OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Organisation for Economic Co-operation and Development, September 23, 1980.
5. Article 76 of the PRC Cybersecurity Law. Please note that the PRC Cybersecurity Law exempts application to military networks which are regulated by separate rules formulated by the Central Military Council of the PRC.
6. *Id*.
7. GB/T 35273-2020.
8. Article 56 of the Draft PRC Personal Information Protection Law.
9. *Id*.
10. EUR-Lex, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62007CJ0518 (accessed 3rd May, 2021).
11. The California Privacy Rights Act of 2020, available at: https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/ (accessed 3rd May, 2021).
12. Cal. Civ. Code § 1798.199.40.
13. Articles 57-61 of the Draft PRC Personal Information Protection Law.
14. See, e.g., Article 58.1 of the GDPR and Cal. Civ. Code § 1798.199.45 *et seq*.
15. Article 3 of the GDPR.
16. See, Lothar Determann, California Privacy Law, 1.2.2.3 (4th Ed. 2020).
17. Article 76 of the PRC Cybersecurity Law; Article 1034 of the PRC Civil Code; Article 4 of the Draft PRC Personal Information Protection Law.
18. Cal. Civ. Code § 1798.140(o); Cal. Civ. Code § 1798.140(v), as amended.
19. 45 CFR Part 160 and Subparts A and C of Part 164; Cal. Civ. Code § 1798.82(a).
20. Article 29 of the Draft PRC Personal Information Protection Law.
21. Special categories of personal data include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning an individual's sex life or sexual orientation. Articles 9 and 10 of the GDPR.
22. Cal. Civ. Code § 1798.410(ae), as amended; § 59.1-571 of the VCDPA.
23. Chapter 2.3 of the Draft PRC Personal Information Protection Law, which provides that the processing of personal information by government agencies in China would be governed by the Draft PRC Personal Information Protection Law and special rules under this Chapter 2.3 thereof.
24. It is however yet clear how broad or narrow this exception of conducting statistical or file management activities by the PRC government agencies would be.
25. Article 68 of the Draft PRC Personal Information Protection Law.
26. Article 2(2) of the GDPR.
27. See, e.g., Cal. Civ. Code § 1798.145 and §§ 59.1-571 and 59.1-578 of VCDPA.
28. Article 1035 of the PRC Civil Code; Article 4 of the Draft PRC Personal Information Protection Law.
29. Article 4(2) of the GDPR.
30. Article 2(1) of the GDPR.
31. Cal. Civ. Code § 1798.140(y) and § 59.1-571 of the VCDPA.
32. See, Determann, L. and Marson, A. (2009) 'Internet business law in China for U.S. Companies', *Computer & Internet Lawyer*, Vol. 13, p. 26.
33. Article 3 of the Draft PRC Personal Information Protection Law.
34. Article 3 of the GDPR.
35. Article 2 of the Draft PRC Data Security Law.
36. See, Determann, L. (2010) 'California Privacy Law, Chapter 2, T and Schwartz, Paul M. and Peifer, Karl-Nikolaus, Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?' *California Law Review*, Vol. 98, p. 1925, UC Berkeley Public Law Research Paper No. 1816885, available at SSRN: https://ssrn.com/abstract=1816885 (accessed 3rd May, 2021).
37. Article 1032 of the PRC Civil Code.
38. Article 12 of the PRC Civil Code.

Book reviews

'Determann's Field Guide to Data Privacy Law: International Corporate Compliance'

By Lothar Determann
Edward Elgar Publishing; Fourth Edition; 2020; ISBN: 978-1-78990-618-9

THE BOTTOM LINE UP FRONT

This is a practical and accessible guide for both privacy practitioners and nonspecialists wishing to understand more of this complex and dynamic subject. In particular, it has wide-ranging utility in the planning and implementation of data protection and privacy compliance in companies operating across the European Union (EU), United Kingdom and/or United States in particular, while also considering the rest of the world (ROW).

The content, format and style enable practitioners to use the field guide as a source of immediate reference. This realistically can answer many of the questions practitioners raise to themselves or have raised by others in their daily duties, while offering simple language that can be easily digested by nonspecialists who wish to understand more.

WHY IS THIS FIELD GUIDE USEFUL

This is the fourth edition to the field guide and has been updated to reflect the dynamic nature of data protection and privacy legislation and to focus on the implications of this, especially when working across multiple jurisdictions. It achieves this by, first, providing a simple baseline of definitions of key concepts, including data protection, privacy and security. This allows communications and the establishment of a shared understanding and discussion of issues and risks to be addressed by privacy professionals and nonspecialists, although from an EU perspective some of the definitions and inferences may be challenged. This leads onto the next two points.

Secondly, it provides a structured approach to addressing the key challenges that privacy professionals encounter in one form or the other — in particular, how to start a compliance program; approach international data transfers; draft appropriate documentation; and maintain and audit compliance programs, including a simple checklist and a simple A–Z data privacy explainer. For many privacy professionals, most of the general concepts and points to be addressed will be familiar, but not necessarily corralled into one place covering different jurisdictions and approaches.

It should be emphasised that the field guide is not a complete how-to textbook, but probably it is best used as a ready reference, to provide practitioners an easily accessible prompt of indicators of good governance, practice and compliance. In providing these indicators, they should be viewed as a representation of the situation only, by providing a short-cut to understanding the more complex reality. But in doing so, this helps practitioners clarify their thoughts and consider how to address issues on a practical basis. For privacy

practitioners starting out in the profession, this is a particularly helpful primer and ready reference that is likely to be used on a regular basis.

Finally, the field guide's content, format and style enable practitioners to step back and use some of the concepts and language as an aide to communicate to nonprofessionals who are not immersed in the subject. By having a shared understanding of the concepts, the indicators of good governance, practice and compliance, privacy practitioners and nonspecialists can have much more meaningful discussions. This should enable much more effective and efficient decision-making, to manage the increasing complex and dynamic privacy environment. In sum, this field guide has a great deal of utility for both privacy practitioners and nonspecialists who wish to understand more about this subject.

Reviewed by Richard Preece