Chambers
Global Practice
Guides

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Cybersecurity 2022

China: Law & Practice
and
China: Trends & Developments

Susan Ning and Han Wu
King & Wood Mallesons

practiceguides.chambers.com

CHINA

Law and Practice

Contributed by:
Susan Ning and Han Wu
King & Wood Mallesons see p.28

CONTENTS

CHINA CONTENTS

1. BASIC NATIONAL REGIME

1.1 Laws

The Civil Code of the PRC (Civil Code) is a periodic legislative response to the problem of personal information (PI) protection. The personality rights chapter of the Civil Code adopts a special section to provide protection on both PI and privacy right, recognising the personality attributes of PI. In addition, the Civil Code preliminarily stipulates the definition and types of PI, the legal basis for processing PI, and the rights of PI subjects, etc. The provisions on PI are periodical and general, therefore remaining to be further refined and implemented by subsequent legislation.

As compared to the scattered provisions set forth by the Civil Code, the Cybersecurity Law (CSL) of the PRC acts as the overarching construct of the cybersecurity regime in China and sets forth specific requirements in various cybersecurity segments. The CSL applies to network operators (NOs) in China, a term defined as any entities that own or administer a network or provide network services, setting forth liabilities of violation in the form of fines and injunctions against the network operators and/or their responsible personnel.

The subject matter regulated by the CSL, supplemented by relevant regulatory documents (including drafts), can be summarised in two main categories: (i) network operation security, which addresses the security of operation, structure and management of a network system; and (ii) network information security, which mainly focuses on measures and structural arrangements to protect PI and important data. The specific requirements of the two categories can be divided into the following major segments.

In addition, the Data Security Law (DSL), which was released on 10 June 2021 and came into effect on 1 September 2021, articulates specific security requirements for data processing. The DSL for the first time explicitly articulates extra-territorial jurisdiction in the Chinese data regulation regime, applying to overseas data processing activities that jeopardise China's national security or the interests of the state or citizens. The DSL contemplates a variety of state data protection mechanisms from an overarching architecture perspective, such as classified data protection system, state data security certification and standardisation, data transaction system, state open data system, and others, with implementation measures to be later promulgated by state and municipal regulatory authorities.

Lastly, the Personal Information Protection Law (PIPL), which was released on 20 August 2021 and became effective on 1 November 2021, building upon the general principles and rules established under the CSL, provides detailed personal information protection requirements. The PIPL, while recognising consent is still the cornerstone of personal information processing activities, provides other lawful bases, such as the necessity for enacting and performing contracts in which the individuals are a party. Additionally, the PIPL put forward requirements in sensitive personal information protection, cross-border transfer, personal information protection impact assessment, compliance audits, separate consent and liabilities.

The CSL, the DSL and the PIPL form the three "pillars" of China's cybersecurity and data protection regime. Moving forward, we expect a series of implementing regulations, measures, and standards to be drafted and finalised.

Network Operation Security

Multi-level protection scheme (MLPS)

A classified cybersecurity protection scheme (also known as the multi-level protection scheme or MLPS) is recognised as the basic legal system to ensure structural network security in China. Under the MLPS, network operators must be classified by one of five levels according to their security impact if the system is damaged, with classification levels ranging from one to five. Progressively stringent requirements for network security and filing obligations with authorities are imposed on network operators at higher MLPS classification levels. Please refer to **4.3 Critical Infrastructure, Networks, Systems** for further details of MLPS.

Security requirements

Certain security requirements are imposed on the suppliers of network products and services, such as taking remedial actions to correct security vulnerabilities and continuing provision of security maintenance services. Any identified key network equipment and specialised cybersecurity product must pass security certification before being put into the market. Network product suppliers and organisations or individuals who detect, collect and publish security vulnerabilities of network products (Vulnerabilities Publishing Platforms) are obligated to report any identified security vulnerabilities to the National Vulnerabilities DataBase. NOs are also encouraged to report such vulnerabilities. Please refer to **5.7 Requirements for Secure Software Development**, "Network Product Security" for further details of the security vulnerabilities.

Critical information infrastructures (CIIs)

Critical information infrastructures (CIIs) are defined as important network facilities and information systems, in industries and sectors such as: telecommunications and information services; energy; transportation; water conservancy; finance; public service; e-government; national defence; science, as well as any other important network facilities and information systems that may severely endanger national security, social welfare and public interests upon sabotage, malfunction or data breach. CIIs are afforded additional and strict security protection requirements and there are obligations regarding security management mechanism, training, technical measures of cybersecurity protection, procurement of network products and services, emergency response plans, and others. As a fundamental principle, protection measures shall be implemented simultaneously when designing, setting-up and using the CIIs.

In addition, in the event that procuring network products and services by CII operators (CIIOs) may affect national security, competent authorities must conduct cybersecurity review of such procurement.

Monitoring, etc

Network operators shall set up cybersecurity monitoring, early warning and emergency response plans to mitigate cybersecurity risks and timely notify relevant parties upon the occurrence of cybersecurity incidents.

Network Information Security

Legitimate processing

NOs shall process (collection, storage, use, handling, transfer, provision, disclosure, deletion, etc) personal information lawfully, legitimately, in good faith, and only to the extent necessary, and obtain informed consent from the PI subjects regarding the purpose, methods and scope of processing. NOs shall also take necessary measures to ensure the security of PI it collects and promptly inform PI subjects and relevant authorities upon discovering possible or identified PI security incidents.

NOs shall take measures to respond to legitimate request from PI subjects related to their

PIs. In particular, based on the PIPL, depending on their different roles in PI processing, NOs are categorised as personal information processors (PIPs) – defined as any entity or individual capable of determining the purpose and method of PI processing – and entrusted processors (EPs) – defined as entities or individuals processing PI on behalf of PIPs.

When PI contains sensitive personal information (SPI), additional security requirements are imposed on PIPs, such as obtaining separate consent and encryptions. Please see **4.1 Personal Data** for details of PI protection requirements for NOs, PIPs and EPs.

Important data

Important data refers to data that may potentially harm national security, economic security, social stability, public health and security, which might include undisclosed government information, information regarding mass population, genetic health, geographical and mineral resources, as well as production and operation information of CIIs. Entities responsible for processing important data are subject to various security obligations under DSL, such as conducting periodic risk assessments and filing the relevant reports as well as adopting technical measures, such as encryption, back-up and monitoring. The scope of important data will be defined by regulatory authorities of different industries and regions in upcoming legislations. Please see **4.2 Material Business Data and Material Non-public Information** for details on important data protection requirements.

Cross-border data transfer

CIIOs must store PI and important data within China and obtain the approval on an authority-led security assessment before transferring such data out of China. PIPs, who processed personal information reaching a threshold to be determined by the Cyberspace Administration of China (CAC), are subject to the same localisation and security assessment requirement. Data processors, defined as those with ability to determine the purposes and means of data processing activities, similarly are subject to the security assessment requirement.

According to the current draft regulations on cross-border data transfer, data processors shall conduct a self-risk assessment before transferring PI and important data cross-border. The self-risk assessment and the authority-led security assessment may cover the nature of data to be transferred, the data recipient's data security protection abilities, the security measures taken to protect data in-transit, the receiving country or region's political and legal environment of data protection, and evaluation of the impact to PI subjects, national security and social interests by such transfer, etc. Cross-border data transfer is prohibited if it threatens national security or public interests. For detailed cross-border data transfer descriptions, please see "Cross-border Data Transfer" under **3.1 De Jure or De Facto Standards**.

The CSL and relevant regulatory documents are mainly enforced by the CAC, the Ministry of Industry and Information Technology of China (MIIT), the Ministry of Public Security of China (MPS), and the State Administration for Market Regulation (SAMR). It is worth mentioning that regulatory documents in drafts are commonly applied as an important reference for cybersecurity enforcement.

State secrets

The Guarding State Secrets Law of PRC ("State Secrets Law") classifies state secrets into three tiers and articulates respective protection requirements, which generally prevail over other data protection requirements when data is identified as a state secret.

Restrictions on state activities
Under DSL and other implementing regulations, governmental authorities bear confidentiality obligations with respect to the personal information, trade secret and other business confidential information disclosed by NOs.

Other laws and regulations
Various other laws and regulations also contribute to other segments of the cybersecurity regime as illustrated below.

The Cryptography Law
The Cryptography Law, mainly enforced by the Cryptography Administration of China (SCA), sets forth requirements for supplying and adopting various encryption, in particular the commercial encryption which plays a key role in network security required by the CSL. The law also sets forth the civil liabilities of violation.

The Provisions on the Ecological Governance of Network Information Contents
The Provisions on the Ecological Governance of Network Information Contents takes network information contents as the main governance objects, and, by aiming at establishing and perfecting a comprehensive network governance system, creates a clean cyberspace and builds a sound network ecosystem.

The Criminal Law
The Criminal Law of the People's Republic of China (Criminal Law) recognises the various cybercrimes infringing PI or computing systems and crimes utilising networks, and the crime of failure to perform cybersecurity obligations, punishable by imprisonment and/or fines. The above-mentioned Criminal Law provisions are enforced by MPS and its local agencies.

1.2 Regulators
All key regulators of cybersecurity in China – namely the CAC, MIIT, MPS and SAMR – have regulatory authorities at the national level and their branch agencies at the county level or above that exercise their authorities within their respective geographic jurisdiction, including audits and investigations of NOs regarding violation of cybersecurity-related laws and regulations.

CAC has the overarching responsibility of planning and co-ordinating cybersecurity regulation. It is the most active regulator in terms of enacting cybersecurity regulatory documents, and its enforcement focuses on the governance of the "internet ecology" and network information content.

The MPS is the key regulator and enforcement authority of the MLPS and network operation security, and responsible for investigating and preventing crimes related to computing system and PI infringement.

The MIIT oversees the telecommunication and information technology industry and thus administers the licences of the market participants in this industry. Its enforcement focuses on PI protection, especially telecommunication value-added services.

The SAMR is responsible for the protection of consumer rights, including consumers' rights in PI and fair market competition.

In addition to the four key regulators, some national regulators focus on specific areas of cybersecurity-related matters, as detailed below.

- The National Security Commission of the Communist Party is responsible for overseeing and formulating state data security strategies under DSL.
- The Ministry of State Security (MSS) is responsible for safeguarding national security of data processing activities.

- The National Information Security Standardisation Technical Committee (TC260) is responsible for the promulgation of cybersecurity-related national standards.
- The National Administration of State Secrets Protection (NASSP) is responsible for MLPS classification and protection related to state secrets.
- The SCA is responsible for regulation and enforcement in relation to encryption activities.
- The China Securities Regulatory Commission (CSRC), the China Banking and Insurance Regulatory Commission (CBIRC), the China Insurance Regulatory Commission (CIRC) and the China Banking Regulatory Commission (CBRC) also regulate cybersecurity matters in their respective financial areas.

1.3 Administration and Enforcement Process

In general, the penalties that cybersecurity regulators or data protection authorities impose on the investigated entities or individuals must comply with the liabilities articulated by the CSL, the DSL, the PIPL and, in case where criminal culpability arises, the Criminal Law.

As for regulator-specific administrative process, the Provisions on Internet Security Supervision and Inspection by Public Security Organs (Public Security Provisions) set forth the standard administrative process of cybersecurity enforcement by the MPS and its branch agencies. The Public Security Provisions limit the scope of the targeted network service providers and the contents of supervision and investigation by public security agencies. It also articulates two methods of supervision and investigation, namely onsite inspection and remote inspection, and sets forth procedural requirements for each method.

Other due process and appeal rights issues not contemplated by the above-mentioned laws and regulations shall, in theory, apply the administration laws of China, namely the Administrative Penalty Law, the Administrative Reconsideration Law, the Administrative Litigation Law, etc. In practice, we are not aware of any remedies under the aforementioned administration laws initiated by respondents. Thus, further observation is advised regarding the applicability of the administration laws to cybersecurity-related administrative process and enforcement.

1.4 Multilateral and Subnational Issues

Currently, most cybersecurity enforcement actions are based on laws and regulations at the national level. Regulations at provincial or municipal level are comparatively limited in number and lack uniformity and consistency in subject matter and legal effectiveness. Although, such regional regulations may only specify but not exceed the requirements already contemplated by the CSL, these regional regulations can shed lights in interpreting the CSL. For example, the Shanghai Public Security Bureau issued the Administrative Penalty Guidance of Cybersecurity Management, setting detailed rules for issuing administrative penalties for violations of the CSL.

Agencies at the subnational level play a piloting and critical role in cybersecurity enforcement activities. For example, the Beijing Cyber Police Department in 2021 launched administrative inspections and issued penalties concerning cybersecurity for 2,775 companies. The Cyber Police Departments of Shanghai and Shenzhen are also very active in launching such inspections on companies of all sizes, including multinational corporations. Furthermore, following the effectiveness of the PIPL, enforcement actions have expanded to include public interest class actions initiated by local Procuratorates. On 1 November 2021, the Hangzhou Internet Court issued its decision for a public interest class action brought by the Gongshu District Procuratorate,

where the defendant was found to infringe the personal information rights and interests.

1.5 Information Sharing Organisations and Government Cybersecurity Assistance

The National Computer Network Emergency Response Technical Team/Coordination Centre of China (CNERT) is a national non-government cybersecurity information-sharing organisation that has played the key co-ordinating role in China's cybersecurity emergency response community since 2001.

CNERT runs the two databases that monitor, alert and provide solutions for information vulnerabilities and malware, namely the China National Vulnerability Database (CNVD) and the Critical Information Infrastructure Security Response Centre (CII-SRC), both of which are joint efforts of information system operators, telecommunication operators, cybersecurity service providers and internet service providers.

In addition, the China National Vulnerability Database of Information Security (CNNVD) is a central government-funded database that has analysed, alerted and responded to information vulnerabilities since 2009.

As required by the Administrative Provisions on Security Vulnerabilities of Network Products (Vulnerability Regulation), the MIIT established the National Vulnerabilities Database (NVDB) in 2021 to collect and publicise the vulnerabilities reported by NOs, network product suppliers and vulnerabilities publishing platforms.

1.6 System Characteristics

While the scope of the cybersecurity regime in China is comparatively comprehensive and diverse in subject matter, it is still under development, with more supplemental measures expected to be released. Cybersecurity enforcement in China has been active and aggressive, especially since 2019, usually focusing in specific areas, such as the mobile application data protection campaign in 2019, 2020 and 2021. Enforcement is expected to expand in scope and enhance in extent in 2022, focusing on app stores and software development kits (SDKs) interpreted within mobile applications. In 2021, the CAC also initiated a series of enforcement actions on public listing on foreign securities markets, namely, the Cybersecurity Review, expanding the scope of enforcement actions.

The cybersecurity legal system in China absorbs some security protection mechanisms from both the US and the EU systems, while maintaining its distinctive designs. For the network security perspective, China affords special protection to CII, a concept derived from the critical infrastructure in both the EU and the US systems; China also sets forth requirements for emergency response, similar to the EU and the US systems. However, the methodology to identify CII and its boundaries in China differs from that used in the EU and the USA; in addition, security requirements for CII is more expansive in China as they are organically connected to other cybersecurity segments, such as security review, MLPS, and cross-border data transfer.

As for data protection, China is similar to most other jurisdictions in the respect that consent of PI subjects is still the cornerstone of PI protection while affording other limited lawful bases, yet it is different in at least four major respects:

- currently, commercial transactions of PI are criminal offences;
- consent by the PI subject is absolutely central to the legal system in China, and thus the dominant source of the lawfulness of PI processing, save for other limited lawful bases provided by the PIPL, such as processing

activities necessary for the compliance of legal obligations;
- the China regime affords additional protection to important data, a concept that the EU or the US systems do not explicitly contemplate; and
- although cross-border data transfer is encouraged, localisation and authority approval is required if regulators deem the transfer may affect national security and public interests.

1.7 Key Developments

In the prior 12 months, a series of key laws and regulations (including drafts) were released or came into force, including the following.

- The DSL was released on 10 June 2021 and came into effect on 1 November 2021. Please see **1.1 Laws** for further information.
- The PIPL was released on 20 August 2021 and came into effect on 1 November 2021, marking China's first comprehensive legislation to define, establish, and integrate the provisions regarding PI protection. Please see **1.1 Laws** for further information.
- The Critical Information Infrastructure Security Protection Regulation (CII Security Regulation) came into effect on 1 Sept 2021, clarifying CII identification rules and providing CIIOs' network protection obligations.
- The Cybersecurity Review Measures was passed in November 2021 and came into effect on 15 February 2022, expanding the scope of cybersecurity review to companies planning to do public offerings in foreign securities markets.
- The Provisions on Several Issues concerning the Application of Law in the Trial of Civil Cases related to the Use of Factual Recognition Technology to Process Personal Information came into effect from 1 August 2021, providing detailed instructions to courts when considering cases involving facial recognition.
- The Algorithmic Recommendation of Internet Information Service Measures, was passed in November 2021 and came into effect on 1 March 2022; this is the first regulation in China that specifically targets the use of artificial intelligence.

As for significant law enforcement activities, the special enforcement campaign against mobile applications illegally collecting and processing PI has discovered thousands of mobile applications infringing PI and ordered violators to rectify accordingly, marking the trend of increasing and extensive enforcement activities by joint forces of regulators. The "Jingwang 2021" campaign against internet-based crimes and PI infringement also marks the continuous strengthening of elevated cybersecurity enforcement by the MPS.

1.8 Significant Pending Changes, Hot Topics and Issues

The CAC released the Network Data Security Management Regulation (Data Security Regulation) for public comments on 14 November 2021, aiming to provide an overarching implementing regulation for the CSL, the DSL and the PIPL. The Data Security Regulation expected to be a game-changer in the cybersecurity and data protection area, because the Regulation would provide clarification in many pending issues, such as:

- the reporting time after identifying security incidents;
- the scope of important data and obligations of important data processors;
- threshold of PI localisation;
- the rights and obligations of data security officers;
- prerequisites of PI portability rights.

Furthermore, measures for cross-border transfer, such as procedures of security assessment

and standard contractual clauses template are also expected to be finalised within 2022.

A number of draft industry-specific regulations and national standards are likely to be finalised this year, such as the draft Data Security Management Measures of Industry and Information Technology Sector (MIIT Data Security Measures) issued by the MIIT.

Hot topics of enforcement emerging since the second half of 2021 include:

- the lawfulness of collecting data from third parties by technical measures, in particular software development kit (SDK);
- processing PI within the scope of necessity, in particular since the release of Provisions on the Scope of Necessary Personal Information of Common Mobile Internet Applications in March 2021;
- the perception of personal information processing activities; and
- cybersecurity review on companies planning (or already) to be listed in the foreign public offering process.

Lastly, sectors such as financial services, automotive and internet services have experience heightened regulatory scrutiny in 2021.

2. KEY LAWS AND REGULATORS AT NATIONAL AND SUBNATIONAL LEVELS

2.1 Key Laws

As mentioned in **1.1 Laws**, the CSL, along with the DSL and the PIPL, lay the foundation of the cybersecurity legal system in China that applies to all kinds of data, systems and information infrastructures, supplemented by a series of implementation measures and other laws and regulations as listed below and sorted by cybersecurity segments.

Network Operation Security

A1: MLPS – Regulation on Graded Protection of Cybersecurity (Draft for Comments) (Draft MLPS Regulations).

A2: CII Protection – CII Security Regulation; Cybersecurity Review Measures, as amended.

A3: Cybersecurity Review and Emergency Response – Cybersecurity Review Measures, as amended.

A4: Encryption – the Cryptography Law and the Law on Guarding State Secrets.

Network Information Security

B1: Personal Information Protection – Civil Code, PIPL, draft Data Security Regulation, Provisions on the Scope of Necessary Personal Information of Common Mobile Applications and Provisions on the Cyber Protection of Children's Personal Information.

B2: Important Data and State Secrets – DSL, Law on Guarding State Secrets.

B3: Cross-border Data Transfer – DSL, PIPL and Cross-border Data Transfer Security Assessment (draft).

B4: Internet Information Content Administration – Provisions on Governance of Network Information Content Ecology, Algorithmic Recommendation of Internet Information Service Measures, Provisions on the Administration of Blockchain Information Services, Provisions for the Administration of Internet News Information Services, and others.

In addition, Articles 253(1), 285, 286, and 287(2) of the Criminal Law apply to the crimes related to cybersecurity.

2.2 Regulators

Please refer to **1.2 Regulators** for their respective responsible area of cybersecurity.

2.3 Over-Arching Cybersecurity Agency

Under Article 8 of the CSL, the CAC is the overarching cybersecurity regulator and agency in China. Please refer to **1.2 Regulators** for its specific regulatory role.

2.4 Data Protection Authorities or Privacy Regulators

The CAC, MIIT, MPS and SAMR at the national level, and their branches at the county level or above, are the major data protection authorities and privacy regulators. Please refer to **1.2 Regulators** for their respective role in data protection. The TC260 is also an important privacy regulator that focuses on the promulgation of data protection-related national standards, and most of the national standards are not legally binding but serve as important reference in legal enforcement activities.

2.5 Financial or Other Sectoral Regulators

The CSRC administers a series of securities-related financial activities in China, including initial public offering (IPO), corporate restructuring, and related transactions. Data compliance of listing companies has become one of the key factors in CSRC approving such activities and contributes to CSRC's rejection of IPO listing application in some cases. In a new draft regulation issued by the CSRC in December 2021, the regulators specifically required issuers to comply with cybersecurity and data protection requirements when planning to be listed in foreign securities markets.

The CBIRC, CIRC and CBRC also regulate cybersecurity matters in their respective responsible financial areas. In particular, the CBIRC takes an active regulatory role, as it issued the Guidelines for Data Management of Banking Financial Institutions in May 2018 and is currently promoting the legislation regarding personal financial information protection. The People's Bank of China (PBOC) is also a key regulator over financial institutions, and released Implementing Measures of the PBOC for Protection of Financial Consumers' Rights and Interests, which came into force on 1 November 2020 as well as the Personal Financial Information Protection Technical Specification, an industry best practice standard.

2.6 Other Relevant Regulators and Agencies

Other key regulators include the NASSP and the SCA, as discussed in **1.2 Regulators**.

3. KEY FRAMEWORKS

3.1 De Jure or De Facto Standards

Key Frameworks

A series of national standards and government announcements have been released. Although some of them were finalised in 2021, many documents are still in draft form for public comments and currently all such national standards are not mandatory. However, in practice a number of these documents are commonly deployed as guidance for law enforcement and corporate compliance, such as the following.

MLPS and network security in general

The Information Security Technology – Baseline for Classified Protection of Cybersecurity (GB/T 22239-2019) (MLPS Baseline Standards) and the Information Security Technology – Classification Guide for Classified Protection of Cybersecurity set forth specifications encompassing the MLPS

classification and evaluation process and the respective requirements for systems at each MLPS classification level. Guidelines on the Protection of Information Security of Industrial Control Systems (ICS Guidelines), promulgated by the MIIT, set forth security protection for industrial control systems (ICS) in various aspects, such as physical environment, authentication, remote access and emergence response.

CIIs

The Information Security Technology – Cybersecurity Protection Requirements of Critical Information Infrastructure (Draft for Comments), the Information Security Technology – Guide to Security Inspection and Evaluation of Critical Information Infrastructure (Draft for Comments), and the Information Security Technology – Indicator System of Critical Information Infrastructure Security Assurance (Draft for Comments) all contemplate the requirements of the identification, inspection, evaluation and security of CIIs.

Emergency response

The National Cybersecurity Incident Emergency Response Plan, promulgated by the CAC, sets forth emergency response measures to various cybersecurity incidents by authorities. The Emergency Response Plan for Cybersecurity Incidents in Public Internet Network, promulgated by the MIIT, sets forth emergency response measures applicable to internet industry participants. The draft Data Security Regulation proposes the time limit as well as procedures for reporting the incidents.

Personal information

The PIPL provides an expanded definition of PI and specifies rules for PI processing activities, PI protection measures and rights for PI subjects. The PIPL is regarded as the fundamental legislation that put in place a key building block of the personal data protection. However, national standard PI Specifications are still practical guidance to PI protection-applicable PIPs and are referred to in data protection compliance practice and enforcement. Guidelines for Internet Personal Information Security Protection, promulgated mainly by the MPS, provides guidance of PI protection tailored to internet companies. Measures for the Identification of Collecting and Utilising Personal Information by Apps in Violation of Laws and Regulations, jointly issued by the CAC, MPS, MIIT and SAMR, sets forth methods of identifying unlawful PI processing by mobile applications. Provisions on the Scope of Necessary Personal Information of Common Mobile Applications, released in 2021, identifies the scope of necessary PI for the basic services of 36 categories and prohibits apps from refusing to provide basic service when users refuse to provide non-necessary PI.

Cross-border data transfer

As mentioned above, under the CSL and the DSL, unless otherwise required by laws and regulations, CIIOs are required to localise PI and important data obtained from operations in China, conduct cross-border transfer of such data only when necessary, perform security assessment requirement beforehand. For general PIPs intended to conduct PI cross-border transfer, pursuant to the PIPL, the PIPs shall inform the PI subjects concerned and obtain their separate consent. The PIPs shall also conduct a personal information impact assessment (PIIA) with regard to the necessity, legitimacy and lawfulness of the transfer, impact on PI subject, security risk and corresponding measures to mitigate the risk. Moreover, PIPs shall satisfy at least one of the following conditions:

- conducting security assessment (if meeting the localisation threshold);
- obtaining PI protection certification by qualified entities;
- entering into standard contracts recognised by the state with the PI receiver; or

- other conditions provided by applicable regulations.

3.2 Consensus or Commonly Applied Framework

The major commonly applied framework for required "reasonable security" are the regulations and national standards related to the MLPS. Please see **2.1 Key Laws** and **3.1 De Jure or De Facto Standards** for further details.

3.3 Legal Requirements

The following illustrate the legal requirements and applicable standards for specific cybersecurity sectors.

Written Information Security Plans or Programmes

China has not established any legal requirements regarding written information security plans or programmes. However, NOs are generally required to provide PI subjects with written documents, usually in the form of privacy policies or consent letters, to inform them of the purpose, methods, and scope of PI collection and processing, the NOs' PI security protection mechanisms, PI subjects' approaches of asserting PI-related claims, risks of PI processing, and others.

Incident Response Plans

The CSL requires that relevant government authorities formulate emergency response plans for their respective industries and fields. Such emergency response plans shall comply with the National Cybersecurity Incident Emergency Response Plan, which classifies cybersecurity incidents into four categories according to their severity and articulates the respective responses to each level. Consistent with the CSL, the DSL requires the competent authority to initiate the incident response plan, take the corresponding emergency response measures, and timely report to the public in the event of a data security incident.

As for private sectors, the PIPL put forward the same obligations by requiring PIPs to formulate incident response plan for PI security incident. It is worth mentioning that, systems classified at MLPS level 2 or above must formulate their own emergency response plans, provide training to its relevant personnel and conduct drills. The Emergency Response Plan for Cybersecurity Incidents in the Public Internet Network also sets forth response requirements for foundational telecommunication companies.

The Data Security Regulation proposes more detailed requirements concerning this mechanism by specifying that PIPs shall notify interested parties and authorities within three working days. Where the incidents involve important data or more than 100,000 individuals' personal information, PIPs shall report to authorities within eight hours.

Appointment of Chief Information Security Officer or Equivalent

Under the CSL and MLPS-related regulations, each NO shall appoint an officer with the general responsibility of overseeing the NO's cybersecurity and MLPS-related arrangements. The CIIOs shall, in addition to appointing such officer, also conduct a security background check of the officer. Further, DSL set out that processors of important data shall appoint a data security officer to be in charge of the data security protection. The PIPL requires a personal information protection officer to be designated if PIPs processes PI reaching a threshold specified by the CAC.

Involvement of Board of Directors or Equivalent

In China, there is no general legal requirement for direct involvement of the board of directors

or equivalent in the cybersecurity matters of a company. However, the fiduciary duty of board of directors under the Company Law of the PRC may give rise to the board's obligations to establish and maintain an effective cybersecurity systems and to take corresponding security measures, depending on the circumstances – for example, the company's affiliated industry or the significance of cybersecurity risks.

The Provisions on the Administration of Informatisation of Insurance Institutions issued by CBIRC require institutions to appoint an executive to be fully responsible for informatisation matters including cybersecurity, under the direct leadership of the board of directors.

The draft Data Security Regulation similarly also propose that the data security officer role shall be assumed by someone at the executive level.

Conducting Internal Risk Assessments, Vulnerability Scanning, Penetration Tests, etc

- MLPS national standards and draft regulations set forth a large variety of risk-assessment requirements, such as periodical security assessments taken by systems at level 3 or above.
- The CII Security Regulations require that the CIIOs establish and maintain a CII risk assessment mechanism and conduct assessment at least annually to rectify security risks discovered in a timely manner and report to the competent authority as required.
- According to the PIPL and other draft regulations, PIPs conducting PI cross-border or DPs transferring important data abroad may be required to conduct security assessments.
- Under the PIPL, as mentioned above, PIPs shall conduct PIIA in certain circumstances such as processing sensitive PI, utilising PI for automatic decision-making, entrusting, sharing, or transferring PI to a third party or publicly disclosing PI, and cross-border transferring PI. The assessment factors shall include the lawfulness, legitimacy and necessity of processing, the risks of adverse effect to PI subjects and the effectiveness of corresponding security measures. The Information Security Technology – Guidance for Personal Information Security Impact Assessment defines the framework, methods and processes of the PI security impact assessment under different scenarios.

Multi-factor Authentication, Anti-phishing Measures, Ransomware, Threat Intelligence

The MLPS national standards set forth a variety of security requirements to network and computing systems, such as:

- systems at level 2 or above shall adopt multi-factor authentication of user identity using passcodes, encryption, biometric technologies and/or other technical measures, in which at least one factor must be encryption; and
- all systems shall install counter-malware software, update malware code database regularly, and establish internal policies of malware countermeasures.

Insider Threat Programmes

The MLPS national standards set forth a variety of security requirements to network and computing systems, such as:

- systems at level 2 or above shall adopt multi-factor authentication of user, in which at least one factor must be encryption; and
- all systems shall install and maintain updated counter-malware software and establish internal policies correspondingly.

Vendor and Service Provider Due Diligence, Oversight and Monitoring

Obtaining PI from vendors and service providers is recognised as indirect collection of PI. The PI

Specifications articulate that PIPs indirectly collecting PI shall request the PI providers to clarify the source of PI, the lawfulness of the source, and the scope of PI subjects' consent, and obtain supplemental consent from PI subjects if the intended processing exceeds the scope of consent.

When PIPs provide their vendors or service providers with PI, their activities constitute the entrusting, sharing, or transferring of PI. The PIPL set forth a series of requirements for such PI provision, such as obtaining informed separate consent from PI subjects, conducting PIIA, contracting with and monitoring PI recipients, and assisting PI subjects to assert lawful requests.

In the event of providing PI to vendors and service providers abroad, PIPs shall ensure the PI would be subject to the same protection level as afforded by the PIPL by satisfying the requirements listed in **3.1 De Jure or De Facto Standards**,"Cross-border Data Transfer".

When procuring network products or services from vendors or providers, under MLPS, the NOs shall ensure that the products or services comply with applicable regulations and standards, and systems at level 3 or above shall conduct inspections before procurement and regularly update and review the list of candidate products. In addition, CIIOs shall ensure that the products or services procured have passed the cybersecurity review by the state if such procurement may affect national security.

Use of Cloud, Outsourcing, Offshoring

The use of cloud is mainly regulated from the MLPS aspect. The MLPS national standards articulate complex and extended security requirements for cloud computing at each MLPS level, covering various aspects of cloud computing security, such as physical environment, network structure, access control, audits, authentication, data integrity and back-up, internal management and service providers. Cloud computing systems at level 2 or above shall maintain their servers physically within China. When the use of cloud involves PI, PICs shall keep such PI physically stored within China.

Outsourcing PI processing is recognised as entrusting, sharing or transferring of PI to third parties. Please see "Vendor and Service Provider Due Diligence, Oversight and Monitoring" (above) for details.

Offshoring mainly concerns cross-border data transfer. Please see the discussion of this topic in **1.1 Laws** for details.

Training

Under the CSL, CIIOs are required to conduct cybersecurity education, technical training and skill assessment for employees on a periodical basis. In line with CSL, both PIPL and DSL demand DPs to carry out personal information protection and data security education and training for the relevant employees on a regular basis. It is worth mentioning that the Data Security Regulation proposes that DPs with important data shall provide no less than 20 hours of data security training for technical and managerial personnel per year.

3.4 Key Multinational Relationships

On 16 September 2021, China sent a formal request to join the regional alliance of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). The CPTPP is the largest regional trade agreement to date, setting out rules on e-commerce to ensure that government regulations in CPTPP markets do not unnecessarily impede cross-border data flows, or impose localisation requirements that force businesses to place data servers in indi-

vidual markets as a condition for serving consumers in that market.

China has entered into Regional Comprehensive Economic Partnership (RCEP) in 2020 covering 15 countries. RCEP establishes regional consensus on cross-border data transfer and limits its members' restrictions on the international digital trades, which facilitates the regional free circulation of data. The RECP has been effective in China since 1 January 2022.

China has entered into bilateral agreements on mutual legal assistance in civil, commercial or criminal matters with a number of countries. These treaties set forth due process requirements of bilateral international legal assistance, which lays the foundation of China's participation in multinational co-operation, such as international co-operation in combating internet-related crimes and frauds.

In addition, China has been actively participating in activities of the establishment of international standards initiated and organised by the International Organisation for Standardisation (ISO).

4. KEY AFFIRMATIVE SECURITY REQUIREMENTS

4.1 Personal Data

The information security requirements in the CSL focus on the following areas – de-identification, secure transmission, deletion and contingency plan. The internal department or personnel in charge of cybersecurity must keep any and all PI, privacy and business secrets obtained during their performance of duties in strict confidence.

Aligned with CSL, the PIPL demands PIPs to take corresponding security measures to ensure the security of PI processed. The aforesaid security measures include: implementing multi-level protection scheme; adopting encryption and de-identification; adopting access control; and formulating an incident response plan. The DSL requires DPs to adopt data security measures covering every step of data processing activities.

De-identification

PI should be immediately de-identified after being collected by PIPs, and technical and managerial measures should be taken to separately store the de-identified data and information that can be used to restore the identification; it should be ensured that no particular individual will be identified during subsequent processing of such data.

Safe Transmission

According to the PIPL and PI Specifications, in principle, PI is not encouraged to be shared or transferred except with a solid legal basis and appropriate safety measures. If sharing or transfer by the PIPs is necessary, PIPs shall perform a PIIA beforehand, obtain PI subjects' separate consent after proper notification, and accurately record the sharing or transferring of PI. Particularly, SPI shall be transferred and stored using encryption and other security measures.

As to the issue of PI cross-border transfer, please refer to **1.1 Laws** ("Cross-border Transfers") for details.

Deletion

PIPs shall take the initiative to delete PI under any of the following circumstances:

- where the purpose of processing has been achieved or is impossible to achieve, the PI is no longer necessary to achieve the purpose;
- where the PIP ceases to provide products or services, or the retention period has expired;
- where the PI subject withdraws consent; or

- where the PIP processes PI in violation of laws, administrative regulations or countersigned agreements.

PI subjects may request the PI to delete relevant PI, if the PIP has failed to do so. Furthermore, where the lawfully mandated minimum retention period has not expired, or the deletion is technically difficult to realise, the PIP shall stop all processing activities except storage and necessary security protection measures.

Emergency Response Plan

Please refer to **3.3 Legal Requirements** ("Incident Response Plans") for details.

4.2 Material Business Data and Material Non-public Information

In general, NO's internal department or personnel in charge of cybersecurity must keep all business secrets obtained during their performance of duties in strict confidence. Data protected by China's cybersecurity regime can generally be divided into categories of PI, important data, trade secrets, commercial encryption and others.

Enterprises are advised to first identify whether its material business data and material non-public information would fall under the definition of PI or important data. If both categories do not apply, such data may, if applicable, fall under the scope of trade secrets, the identification and protection of which are set forth by the Anti-Unfair Competition Law of the PRC.

For security requirements of business data or non-public information identified as PI, please refer to **4.1 Personal Data**.

If material business data is recognised as important data, according to the CSL, NOs are required to take measures such as back-up and encryption of important data. Besides, the DSL also provides the protection system for important data. Article 21 states that each region and department shall formulate the specific catalogue of important data for the region, department, related industry and sector, and focus on the protection of data listed. Article 27 (2) further mandates important data processors to appoint a data security officer and set up a management institution in charge of data security. Article 30 requires such processor to carry out risk assessment on data processing activities on a regular basis, and submit the risk assessment report to the relevant competent department. Additionally, the draft Data Security Regulation as well as the draft Data Security Management Measures for Industry and Information Technology Sector both propose that important data processors shall file the identified important data with the competent authorities.

Various requirements are imposed by the Cryptography Law when enterprises adopt commercial encryption to protect data. The commercial encryption products closely related to national and social public interests shall be certified by qualified inspection agencies before marketisation. CIIOs adopting commercial encryption shall conduct security assessments by themselves or by qualified inspection agencies. When CIIOs' procurement of network products or services adopting commercial encryption may affect national security, a security review of the procurement shall be conducted by relevant state authorities.

4.3 Critical Infrastructure, Networks, Systems

Under the MLPS, in principle NOs are required to:

- formulate internal security management systems and operation instructions to determine the person in charge of cybersecurity and define accountabilities for cybersecurity;

- take technical measures to prevent computer viruses, network attacks, network intrusions and other activities that endanger cybersecurity;
- monitor and record network operation and cybersecurity events, and maintain cyber-related logs for no less than six months as required; and
- take measures such as data classification, back-up and encryption of important data.

MLPS protects generic information networks, ICS, cloud computing platforms, internet of things (IoT), big data platforms, mobile communication systems and others network systems (MLPS subjects). NOs have different filing and self-assessment obligations for their MLPS subjects at each of the five protection levels – the higher level the classification is, the higher compliance obligations the NOs have.

In addition to the above requirements applicable to all NOs, CIIOs are in principle identified as level 3 or above, and have additional general obligations to:

- establish a dedicated security management department, appoint a cybersecurity officer, and carry out security inspection of such cybersecurity officer and people in key positions;
- provide periodic cybersecurity education, technical training and assessments for its employees;
- maintain back-up for important systems and databases in anticipation of catastrophes; and
- formulate emergency response plans for cybersecurity breach incidents and conduct periodic drills.

In the scenario of cross-border data transfer by CIIOs, please refer to **1.1 Laws** ("Cross-border Transfers") for details.

In addition, the CII Security Regulations further specify the requirements on the security protection of CII, encompassing the identification of CIIs, response to security incidents, daily operation and security maintenance, security monitoring and inspections, security assessment security of network products and services procurement, and others.

Following the issuance of the Practical Guide to the Multi-level Protection Scheme and Critical Information Infrastructure Security Protection System (Practical Guide) by MPS, the basic framework of CII protection will be gradually set by series of supporting standards, including the identification, security, monitoring and warning, testing and evaluation and incident handling of CII, and important industries and sectors will simultaneously make preliminary progress in establishing the CII identification mechanism based on characteristics of each sector. Overall, the regulatory efforts focus on the CIIOs' obligation of multi-level assessment and CII protection.

4.4 Denial of Service Attacks

Apart from the general security requirements for NOs under the CSL – described in **4.3 Critical Infrastructure, Networks, Systems** – the Draft MLPS Regulations contemplate general MLPS monitoring requirements related to preventing denial of service attacks. Particularly, while NOs shall monitor and record their network security status, operators of MLPS subjects at level 3 or above shall in addition adopt further precautionary and monitoring measures and timely file the results with local public security bureaus.

With regard to the technical specifications of preventing denial of service attacks, the MLPS Baseline Standards prescribe respective requirements for MLPS subjects at each level regarding the security protection capacity in the four key technical aspects: secure management centre,

secure network, safe regional boundary and safe calculation environment.

4.5 Internet of Things (IoT), Software, Supply Chain, Other Data or Systems

Apart from overarching guidelines in the CSL and supporting regulatory documents, there are laws and regulations in particular industries or sectors that also touch on the topic of cybersecurity, as exampled below.

- The Law of the People's Republic of China on Guarding State Secrets mandates that hierarchical protection measures shall be adopted for the computer information systems which are used for storing or processing state secrets and organs and agencies shall enhance their control over the secret-involved information system.
- The Administrative Regulations on Maps prescribes that entities engaging in internet map services shall establish the management system as well as protection measures for the data security of internet maps.
- According to Measures for the Administration of Population Health Information (for Trial Implementation), population health information shall be subject to hierarchical storage. Entities in charge shall establish a reliable working mechanism for disaster back-up of population health information, and conduct back-up and recovery inspections on a regular basis.
- The Cybersecurity Review Measures requires CIIOs to conduct cybersecurity review prior to the purchase of network products and services that affects or may affect national security to ensure the supply chain security of critical information infrastructure and safeguard national security. It also applies to data processing activities by online platform operators when the processing activities impact or may impact national security.

5. DATA BREACH REPORTING AND NOTIFICATION

5.1 Definition of Data Security Incident, Breach or Cybersecurity Event

According to the National Cybersecurity Incident Emergency Response Plan, "cybersecurity incidents" refer to incidents that cause harm to the network and information systems or data therein and adversely affect society due to human factors, hardware or software defects or failures, natural disasters, etc. They can be categorised as hazardous program incidents, network attack incidents, information destruction incidents, information content security incidents, equipment and facility failures, catastrophic incidents, and other incidents. Furthermore, cybersecurity incidents are graded into four levels, namely: severely material, material, relatively material and general cybersecurity incidents.

5.2 Data Elements Covered

For the purpose of data security incident or breach regulations, generally all types of data may be covered. In addition to general types of protected data – namely, PI, important data, trade secrets and data contemplated under the National Cybersecurity Incident Emergency Response Plan – other data that may be covered include state secret information, important sensitive information, critical data or other data whose loss would pose certain threats to or have certain impacts on national security, social order, economic construction and public interests.

5.3 Systems Covered

The legal construct of data security incident or breach covers:

- systems involving important network and information systems that undertake business closely related to national security, social

order, economic development and public interest; and
- network and information systems that would pose threats to or incur impacts on national security, social order, economic construction and public interests upon being damaged.

5.4 Security Requirements for Medical Devices

The Guidelines for Technical Review of Medical Device Network Security Registration articulate general security requirements for the applicants for medical device network registration, such as:

- paying continuous attention to cybersecurity issues during the whole life cycle of medical device production;
- perfecting the user access control mechanism; and
- notifying users of relevant cybersecurity information in a timely manner.

5.5 ecurity Requirements for Industrial Control Systems (and SCADA)

The fundamental security requirements for ICS (including SCADA) can be found in the ICS Guidelines which list 11 protection requirements, covering:

- security software selection and management;
- configuration and patch management;
- boundary security;
- physical and environmental security;
- identity authentication;
- remote access security;
- security monitoring and emergency drills;
- asset security;
- data security;
- supply chain management; and
- responsibility implementation.

In addition, the MLPS Baseline Standards provide security requirements specifically for ICS, such as outdoor control equipment protection, network structure security, dial-up usage control, wireless use control and control equipment security. The Guidelines for Categorisation and Classification of Industry Data (Trial), circulated by the MIIT, put forward preliminary guidance on categorising data in combination with industrial manufacturing models and service operation models, and graded the industrial data into three levels by considering the potential impacts on industrial production and economic benefits after different types of industrial data are distorted, destroyed, disclosed or illegally used.

5.6 Security Requirements for IoT

MLPS Baseline Standards provide security extension requirements for IoT such as the physical protection of sensor nodes, device security of sensor nodes, device security of gateway nodes, management of sensor nodes and data fusion processing. Other national standards also serve as reference for IoT security, such as the security technical requirements for data transmission.

The Guidelines for the Construction of Basic Security Standard System of Internet of Things 2021 puts forward the framework of the basic security standards, key standardisation fields and directions of the basic security of IoT, including overall security requirements, terminal security, gateway security, platform security and security management.

The Guidelines for Construction also proposed to set up the basic security standard system of the IoT in 2022 and promoted the formation of a relatively complete system of IoT basic security standards in the next three years. It specifically defined the security requirements for key basic fields such as IoT terminals, gateways and platforms. The requirements include system construction, safety organisation, personnel management, operation safety, asset management, configuration management, remote

maintenance safety, vulnerability detection, emergency response, and management and disaster recovery.

5.7 Requirements for Secure Software Development

Certification

Administrative Measures on Testing and Sales Permits for Products Dedicated for the Security of Computer Information Systems released by MPS in 1997, proposed that the term "*the products dedicated for the security of computer information systems*" shall refer to the hardware and software products dedicated for the security of computer information systems. Selling security dedicated products in China is subject to the sales permit system.

Furthermore, Implementing Measures on Security Certification for Critical Network Equipment and Specialised Network Products provides that the specialised products for network security require security certification. The specialised products for network security are divided into 15 categories, according to the Catalogue of Critical Network Equipment and Network Security Products (First Batch) 2017, including WAF, IDS, IPS and network comprehensive audit system.

Network Product Security

The Vulnerability Regulation requires network product suppliers, Nos, and vulnerability publishing platforms to establish unimpeded channels for receiving vulnerability information, and timely verify and complete the repair of vulnerabilities. Meanwhile, the Vulnerability Regulation also provides specific time periods for network product suppliers to report vulnerabilities and their obligations to provide product users with technical support. For vulnerability publishing platforms, the Vulnerability Regulation specifies eight requirements, such as allowing them to disclose product vulnerabilities in advance upon assessment and negotiation, prohibiting them from releasing details of network operators' vulnerabilities, simultaneously releasing remedial and preventive measures, and prohibiting them from providing undisclosed vulnerabilities to overseas organisations or individuals other than product providers

5.8 Reporting Triggers

Government Authorities

Under the Cybersecurity Law, concerned NOs shall report incidents that threaten cybersecurity to the competent authority. For instance, the following.

- The Automotive Data Security Management Measures requires the automotive data processor that conducts important data processing activities shall, before 15 December of each year, submit the annual automotive data security management report, including the automotive data security incidents and the handling thereof, to the provincial CAC and relevant authorities.
- The Promulgation of the Administrative Measures on Regulatory Data Security (Trial Implementation), issued by the CBIRC, prescribes that in case of occurrence of significant security risks relating to regulatory data, the business department or entrusted organisation concerned shall immediately take emergency response measures and report to the Statistics Information Department of the CBIRC within 48 hours.
- According to Regulations of the PRC on the Security Protection of Computer Information System, users of a computer information system shall report any case arising from such system to the local public security bureau at county level or above within 24 hours.
- The Telecommunications Regulations of the PRC prescribe that telecom operators shall report to the relevant national authorities upon discovery of illegal transmission of information contents as described in Article

56 in the course of their public information services.
- The draft Data Security Regulation proposes that for any data security incident – such as leakage, damage or loss – DPs shall report to interested parties within three business days. Where important data or more than 100,000 individuals' personal information is involved, the DPs shall report to the municipal CAC and relevant authorities within eight hours of the occurrence of the security incident. DP should also submit an investigation and assessment report covering the cause of the incident, the consequence of harm caused, the accountability and the improvement measures taken, among other information, to the district city-level cybersecurity authority and other relevant authorities within five business days of the disposal of the incident.

As for CII, authorities in charge shall establish the cybersecurity monitoring mechanism and information reporting mechanism for specific industries/sectors within their respective jurisdictions.

In case of increasing risk of cybersecurity events, governments at provincial level and above shall take measures to require authorities, agencies and personnel concerned to promptly collect and report necessary information and enhance monitoring of cybersecurity risks.

In accordance with the CSL, PIPL and DSL, China has established a national cybersecurity information reporting mechanism led by the CAC and MPS, while multi-ministries/bureaus – including MIIT, NDRC and the secrecy bureau – are also participating.

Individuals
Under the CSL, in case of disclosure, damage or loss (or possible disclosure, damage or loss), NOs are obligated to notify the affected users promptly. In addition, for any risk, such as security defect or bug in network products or service, the product/service providers concerned shall inform the users of such risk. In addition, according to the PIPL, in case of PI security incident, affected PI subjects shall be notified of information related to the incident.

Other Companies or Organisations
Duty to report to other companies may be triggered by contractual obligations.

Industry organisations may determine reporting obligations to its members, under Article 29 of the CSL. Other industry self-regulated obligations to report to information-sharing organisations, as described in **1.5 Information Sharing Organisations and Government Cybersecurity Assistance**, may also exist.

5.9 "Risk of Harm" Thresholds or Standards
There are various thresholds and standards of notification in China's cybersecurity regime.

For instance, according to the Emergency Response Plan for Cybersecurity Incidents in Public Internet Network, the lowest level of network security incident is the general network security incident which shall suit one of the following conditions:

- a large number of internet users within one municipality are unable to access the internet normally;
- the leakage of the information of more than 100,000 internet users; and
- other incidents that cause or may cause general harm or effect.

It could be implied at least the same level of threshold of cybersecurity harm is applicable to data breach incident notification.

In addition to the harm to cybersecurity, notification obligations are also triggered when personal information is "likely to be divulged, damaged or lost" under the CSL.

6. ABILITY TO MONITOR NETWORKS FOR CYBERSECURITY

6.1 Cybersecurity Defensive Measures

According to the Measures for Monitoring and Handling Threats to the Cyber Security of Public Internet, telecommunications authorities (including MIIT and provincial communication administrations) are in charge of monitoring cybersecurity threats. Thereafter, Information Security Technology – Basic Requirements and Implementation Guide of Network Security Monitoring 2018 sets out the framework and baselines for network security monitoring, which contemplate that network security monitoring are conducted through real-time collection of network and security equipment logs, system operation data and other information.

6.2 Intersection of Cybersecurity and Privacy or Data Protection

The intersection of cybersecurity and privacy illustrates the conflict arising from the intertwined interests of the community and of individuals/entities. For instance, from the commercial practice perspective, as companies impose confidentiality obligations on their employees, an employee reporting the vulnerability of his or her company's network system to a third party is in conflict with their confidentiality obligations.

Although it is difficult to clearly define the boundaries between the two, the state tries to balance the scales. For example, in the PIPL, the processing of PI by state organs to perform their statutory functions shall be carried out in accordance with the authority and procedures provided in laws and administrative regulations, and shall not exceed the scope and limits necessary for the statutory functions, which means public authorities may only collect and use personal information upon data subjects' authorised consent or statutory authorisations by laws or administrative regulations, even when cybersecurity threat is involved. Generally speaking, we understand that only circumstances of certain criminal investigations or threats to national security may trigger such statutory authorisation.

Additionally, under the CSL, DSL, PIPL, and the implementing regulations, authorities and their staff bearing relevant regulatory authority must carefully keep strict confidentiality of any PI, privacy information and business secrets obtained in their performance of duties. Furthermore, Article 30 of the CSL prescribes that cyberspace administrations and authorities concerned shall only use the information accessed in performance of their duties for cybersecurity protection purposes.

7. CYBERTHREAT INFORMATION SHARING ARRANGEMENTS

7.1 Required or Authorised Sharing of Cybersecurity Information

Please refer to **5.8 Reporting Triggers** ("Government Authorities") for details of this matter.

7.2 Voluntary Information Sharing Opportunities

With regard to Article 29 of the CSL, the state supports the co-operation among network operators in collection, analysis and notification of cybersecurity information and emergency response, in order to improve their cybersecurity protection capacities. The relevant industry organisations shall establish and improve respective cybersecurity rules and co-ordination

mechanisms, enhance analysis and assessment on cybersecurity risks, regularly release risk alerts to their members, and assist their members with coping with cybersecurity risks.

In China, users, suppliers and research institutions are encouraged to report any potential system vulnerabilities identified to the CNVD, as described in **1.5 Information Sharing Organisations and Government Cybersecurity Assistance**, so as to gather, verify and warn against any security vulnerabilities and to establish an effective and co-ordinated emergency response mechanism among all operators.

Also, there are scenarios where system vulnerabilities shall be mandatorily reported, as described in **5.7 Requirements for Secure Software Development**.

It is worth noting that a major cloud service provider had been suspended by MIIT, with their partnership ending in 2021, because of failing to meet the mandatory reporting obligation.

8. SIGNIFICANT CYBERSECURITY AND DATA BREACH REGULATORY ENFORCEMENT AND LITIGATION

8.1 Regulatory Enforcement or Litigation

In the field of administrative supervision, app governance is still the most important work for regulatory authorities in the field of data protection in 2021. MPS further promoted the special action of "Jingwang 2021" and achieved remarkable phased results, with more than 37,000 illegal activities related to network being detected. In the meantime, MIIT issued a notice on launching actions for improvements to the perception of information and communications service. It is required to establish the list of collected personal information and a list of personal information shared with third parties, and display the same in the secondary menu of the app.

As of September 2021, MIIT has issued a total of 19 batches of "app notification on infringement of user rights", of which five batches were issued in 2021. The notified apps concern many fields, and the listed problems focus on the illegal collection of PI compulsory access to authority, etc.

8.2 Significant Audits, Investigations or Penalties

Since last year, the regulatory authorities have significantly strengthened their supervision over the protection of personal information security. The CBIRC released an administrative penalty notice on its official website, indicating that China CITIC Bank received a fine of CNY4.5 million for several violations of laws and regulations, such as enquiring about and then providing transaction information of a customer's personal bank account to a third party without the authorisation of the customer.

The PBC has issued more than 31 penalty decisions involving personal information security (including institutions and individuals). Most of the punishment decisions are for the violation of enquiring about personal information without the subject's consent, including enquiring about individual credit reports or loan information without the subject's consent and negligent disclosure of personal information.

8.3 Applicable Legal Standards

Please refer to **1.3 Administration and Enforcement Process** and **1.4 Multilateral and Subnational Issues**.

8.4 Significant Private Litigation

A WeChat user filed a lawsuit, claiming that the Weishi app (operated by Tencent) used the plaintiff's personal information in WeChat without authorisation, including region, gender and WeChat relationship. Upon trial of the second instance, the court held that the Weishi App's compulsory acquisition of the user's region and gender information did not satisfy the principle of necessity of collecting user information.

Further, in the scenario that the plaintiff uninstalled the Weishi App and re-used the same account to log in to the Weishi App without consent and authorisation, the user had reasonable grounds to believe that it no longer authorised the Weishi App to use the WeChat friend relationship. Weishi's continuous use of the stored WeChat friend relationship in the back-end did not meet the user's "reasonable expectation" of the consequences of his authorisation. Therefore, the Weishi App's continuous use of the plaintiff's WeChat friend relationship did not meet the lawfulness principle when the plaintiff downloaded the app for the second time.

8.5 Class Actions

Article 70 of the PIPL establishes the foundation of public interest litigation for the protection of personal information. The Procuratorate, the consumer organisation as provided by law, or the organisation determined by the CAC may file a lawsuit with the court in accordance with the law. In addition, the Supreme People's Procuratorate (SPP) promulgated the Circular on Implementing the Law on the Protection of Personal Information and Promoting the Procuratorial Work of Public Interest Litigation on the Protection of Personal Information, clarifying the key points of handling public interest litigation on the protection of personal information.

9. DUE DILIGENCE

9.1 Processes and Issues

The process of diligence in corporate transactions mainly concerns the security and the asset aspects of data.

For the security aspect, MLPS classification and evaluation of a company's information system are the first steps of due diligence. Comprehensive assessments of cybersecurity based on MLPS classification will then be conducted to perform gap analyses of various security-related matters, including emergency response, PI protection, cross-border data transfer security and CII protection.

As for the asset aspect, due diligence will focus on confirming the legitimacy of the corporate data and identifying the legal boundary of corporate data assets. As security and compliance of data are the premises of data assets, taking data mapping as reference, assessment reports will be issued to review the corporate compliance of data regarding various matters, such as PI processing, internal corporate systems related to cybersecurity and data compliance, information content administration, and others. Identifying the boundary of the company's data and the claims the company has over them will be the next step to confirm the company's proprietary rights on the corporate data.

9.2 Public Disclosure

The National General Response Plans for the Public Emergency Incidents set forth local government authorities' obligations to report public emergency incidents to higher level authorities. Cybersecurity risks that constitute a public emergency incident may be disclosed and reported to various level of authorities for emergency alerts and responses. The Emergency Response Law of the PRC also requires that all entities shall timely report their potential emergency incidents

to local authorities in accordance with applicable laws and regulations. In the financial area, the Measures for the Administration of Initial Public Offering and Listing of Stocks and other similar IPO administration measures require that any information that may have any major impact on the investors' decisions on investment shall be disclosed in IPO prospectuses.

However, entities should note that the disclosure of cybersecurity information may be subject to certain limitations under recent draft measures by the CAC, as described in **1.5 Information Sharing Organisations and Government Cybersecurity Assistance**.

10. INSURANCE AND OTHER CYBERSECURITY ISSUES

10.1 Further Considerations regarding Cybersecurity Regulation

Considering the extraterritorial jurisdiction of PRC cybersecurity regulations, "domestic operation" also entails an enterprise's acts that are intended to provide goods or services to individuals within the PRC.

King & Wood Mallesons is an international law firm headquartered in Asia with a global network of 27 international offices. KWM's cybersecurity team is one of the first legal service teams to provide professional services concerning cybersecurity and data compliance in China; it consists of more than ten lawyers with solid interdisciplinary backgrounds, mainly located in Beijing, while further specialisms are found within KWM's global network. The team has expertise in assisting clients in responding to cybersecurity inspections and network emergencies, the establishment of network information compliance systems, self-assessment, internal training on cybersecurity and data compliance, and other related matters. Recently, KWM advised a renowned short-term lodging platform on compliance with the multi-level protection of cybersecurity, during which KWM provided elaborative analysis on the current graded protection obligations and further comparatively analysed the newly proposed mechanism and the existing one, thereby enabling it to offer practical advice to the client.

AUTHORS

Susan Ning is a senior partner and the head of KWM's regulatory group. She is one of the pioneers engaged in cybersecurity and data compliance practice, with publications in a number of journals, such as the "Journal of Cyber Affairs". Her publications include "Big Data: Success Comes Down to Solid Compliance" and "No Data, No Internet of Vehicles". Susan's practice areas cover self-assessment of network security, responding to network security checks, data compliance training, etc. She has assisted companies in sectors such as IT, transportation and finance in dealing with network security and data compliance issues.

Han Wu is a partner of KWM's regulatory group. He excels in providing cybersecurity and data compliance advice to multinationals' Chinese branches and in establishing network security and data compliance systems for Chinese enterprises operating abroad. In the areas of cybersecurity and data compliance, Han provides legal services, including assisting clients in establishing a cybersecurity compliance system, self-investigation on cybersecurity, network security investigations, cybersecurity incidents, data fusion and identification of data assets. Han has provided legal services on cybersecurity and data compliance to companies in multiple industries. The projects in which he has participated encompass the financial payments, consumer electronics, internet advertising and healthcare industries.

King & Wood Mallesons

18th Floor, East Tower,
World Financial Center
1 Dongsanhuan Zhonglu
Chaoyang District
Beijing
100020, PRC

Tel: +86 10 5878 5588
Fax: +86 10 5878 5566
Email: kwm@cn.kwm.com
Web: www.kwm.com

Trends and Developments

Contributed by:
Susan Ning and Han Wu
King & Wood Mallesons see p.36

Overview

The year 2021 marked a significant development in China's cybersecurity and data protection legislative regime. The long-awaited Data Security Law (DSL) and the Personal Information Protection Law (PIPL) were both finalised and came into effect in 2021. These two laws, together with the Cybersecurity Law (CSL), which has been effective since 2017, form the overarching legislative framework of cybersecurity and data protection.

Regulators also finalised many implementing regulations. For example, after seven months of public consultation and deliberation, the Cybersecurity Review Measures (CRM), as amended, came into force on 15 February 2022, signalling that China's cybersecurity enforcement has moved into a new era. The CRM mandates that (i) critical information infrastructure operators (CIIOs) procuring network products and services, and (ii) network platform operators carrying out data processing activities that affect or may affect national security shall be subject to cybersecurity review organised by the competent authorities.

Another example is the Critical Information Infrastructure Security Management Regulation ("CII Security Regulation"), which was adopted on 1 September 2021; it lays down the fundamental security compliance obligations for CIIOs, ensuring the CIIOs are well protected in cyberspace.

A series of implementing regulations are expected to be released or finalised in 2022. Aside from the traditional cybersecurity regulations, regulators in various industries are expected to issue cybersecurity-related regulations focusing on industry-specific issues. These regulations are expected to address pending issues and provide more practical guidance.

As such, the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law (albeit with certain specific compliance requirements) generally act as fundamental laws, while regulators in each industry are tasked to promulgate respective implementing regulations.

The Data Security Law

The Data Security Law (DSL) that came into effect in September 2021 represents the legislation's first effort at the state level to regulate data processing activities by balancing the security and the utilisation aspects. The DSL provides the fundamental legal basis for the Cyberspace Administration of China (CAC) and other competent authorities to ensure data processing activities do not harm state security, public interests and private interests.

The DSL contemplates extraterritorial jurisdiction over offshore data activities affecting state security, public interests and private interests within the PRC; it operates in conjunction with the Cybersecurity Law (CSL) in many areas. For instance, the DSL requests data processors to perform data security protection on top of the multi-level protection scheme as prescribed by the CSL.

The DSL contemplates a general principle of data categorisation and classification based on the importance of data and the damage incurred upon data breach. Some industry regulators have issued national and industry standards for

their respective sectors, such as finance and healthcare. In December 2021, the National Information Security Standardisation Technical Committee (TC260) issued the Cybersecurity Standard Practical Guidance – Network Data Categorisation and Classification, a non-binding guideline, which provides general and universal guidance on conducting data categorisation classification.

The DSL requires governments at different levels to issue catalogues of important data to identify and provide heightened protection to such data, including periodical risk assessment. Although there have been several attempts to provide straightforward criteria, the specific scope of "important data" is to be determined. The new draft regulations now propose to require data processors to self-identify important data and then file the identification result with the industry regulators. Hence, it is likely that the scope of important data will become clearer in 2022 or early 2023.

The DSL requires that data security reviews should be conducted on data processing activities that may affect state security. Although the cybersecurity review system has been established, the data security review is a different review process. The implementing regulation thereof is likely to be issued in the new future.

The Personal Information Protection Law

The Personal Information Protection Law (PIPL) came into effect in November 2021. While primarily focusing on protecting personal information (PI), the PIPL also supplements the network information security requirements under the CSL.

In essence, the PIPL aims to work as an independent legislature specifically focused on PI protection, which significantly changed under the CSL. The PIPL contemplates extraterritorial jurisdiction over offshore processing of the PI of natural persons within the PRC if the action is intended to provide goods or services to such person or assess such person's behaviour. This illustrates the legislation's response to the trend of extraterritorial jurisdiction worldwide, such as the GDPR in the EU and the CCPA in the USA, to afford individuals within the PRC equal protection. Foreign companies should be mindful of the extraterritorial jurisdiction when dealing with individuals within the PRC.

The PIPL lines up with the terminology used in the Civil Code, and defines the entity or individual capable of determining the purpose and methods of PI processing as the "PI processor", rather than the "controller" concept used in other jurisdictions such as the EU. In addition, the "entrusted processor" under the PIPL is comparable to the "data processor" in the GDPR.

Besides the consent and requirement laid down by other laws and regulations, the PIPL introduces additional legal bases including:

- necessity for executing or performing contracts where the individual is a party;
- necessity for human resources management based on lawfully enacted labour rules and collective bargain agreements;
- protection of public health in an emergency; and
- certain reasonable acts to protect the public interest.

It is a drastic expansion from the CSL's framework, and grants enterprises much more flexibility.

The PIPL also introduces the first attempt to regulate the cross-border transfer of PI by general entities at the statute level, compared to the cross-border transfer provisions applicable to CIIOs in the CySL. Specifically, it extends the

scope of data localisation and mandatory security assessment for outbound PI transfer, previously only applied to transfers conducted by CIIOs, to mass-volume PI processors (the standard is to be determined by regulators). For transfers conducted by other entities, it also provides several new approaches of compliant outbound PI transfer as compared to the sole approach of security assessment under the current cross-border security transfer rules. In general, foreign enterprises processing a large volume of user data may incur legal risks if providing service to PRC users without deploying the server within the PRC. It also requires PI processors to obtain independent consent from PI subjects, which is different from explicit consent under the GDPR.

In sum, the PIPL reflects the legislation's attitudes and objectives in PI protection that elevates requirements for PI protection while endeavouring to strike a nuanced balance between PI rights and market participants' interests in processing PI in the evolving era of the digital economy.

The Draft Network Data Security Management Regulation

In order to harmonise the requirements under the CSL, the DSL and the PIPL, the CAC released the draft Network Data Security Management Regulation ("Data Security Regulation") on 14 November 2021. This Regulation proposes to implement the high-level instructions contained in the aforesaid laws. For instance, the laws all require companies to develop an emergency plan for security incidents and report the incidents to the competent authority, but do not specify the time limit of the reporting obligation. The Data Security Regulation proposes that if a security incident has caused harm, companies shall notify the interested parties within three business days. Moreover, if the security incident involves important data or more than 100,000 individuals, the companies shall report to competent authorities within eight hours upon the occurrence of the security incident.

Although filled with detailed contents, duties imposed by the Data Security Regulation can be generally categorised into four aspects: record, assessment, review and filing/report in relation to data processing activities, which provide regulators with regulatory tools that are practical and down-to-earth. For example, as evidenced by the automotive industry, after the local MIIT branches received the annual automotive data security report, the regulator would approach the companies to discuss high-risk data processing activities and request remedial measures.

However, if the Data Security Regulation is finalised as is, companies may face unprecedented compliance burdens. Therefore, the draft Regulation has led to heated discussions, and many proposed requirements are likely to be modified. However, the Regulation provides valuable insights into the CAC's view of how companies should manage data processing activities.

Cybersecurity Review

As a crucial aspect of national security review, a cybersecurity review was enacted to protect national security interests by examining the network products or services to be procured by CIIOs, whose network products and associated information systems, by definition, may have national security interests.

In July 2021, the CAC issued an amendment to the CRM, expanding the scope of cybersecurity review to data processing activities that may affect national security. Particularly, because public offerings in foreign securities markets involve a significant volume of cross-border data transfers, the amendment requires data processors, who possess more than one million individuals' personal information, to proactively file for a cybersecurity review when planning to be

listed in a foreign security market. The amendment was passed in November 2021 and came into force on 15 February 2022. Although the finalised CRM changed the terminology from data processors to network platform operators, it is likely that these terms have similar scopes.

The cybersecurity review focuses on two aspects. The first aspect is the procurement of network products or services by CIIOs, including:

- the risk of any CII being illegally controlled, tampered with or harmed after using the network products or services;
- the risk of any CII's supply of network products or services being interrupted;
- the security, openness, transparency, diversity of sources and reliability of the supply channels of network products or services, as well as the risk of the supply chain being interrupted due to political, diplomatic, trade or other factors; and
- the compliance situation of the suppliers with the RPC laws and regulations.

The second aspect is data processing activity, including: the risk of core data, important data or a large volume of personal information being stolen, leaked, destroyed and illegally used or transferred abroad; the risk, during and after the public offering, that CII, core data, important data or a large volume of personal information might be affected, controlled or maliciously used by foreign governments, as well as any network information security risk.

The cybersecurity review process may take a month to complete if it is initiated by the Cybersecurity Review Office (CRO) under the CAC, but when a CIIO or a network platform operator proactively applies for cybersecurity review, the CRO should conduct a pro forma review and notify the applicant in writing whether or not a full-blown cybersecurity review will be conducted within ten business days upon receiving application materials.

It is worth noting that it is not clear whether CRM is applicable to foreign companies. Based on the legislative intent of mitigating risks incurred by data processing activities, it is still likely that the CAC may require such a foreign company to file for a cybersecurity review if the company has a significant operation in China.

Multi-level Protection Scheme (MLPS)

The MLPS requirements and standards generally remained the same in the year of 2021, but the draft Data Security Regulation proposes that all systems processing important data must be qualified as MLPS level three, creating an interoperative link between cybersecurity and data security.

Additionally, we have observed that an increasing number of multinational companies (MNCs) are considering conducting MLPS. This trend suggests that these companies partially localised their networks because MLPS can only be conducted for domestic networks.

The CII Security Regulation

Section 2 of the CSL has envisaged a framework of operation security of CII by setting out basic principles, imposing basic security protection obligations on CIIO, and requesting localisation of the PI and important data collected by CIIO.

In line with the CSL, the CII Security Regulation lays down detailed responsibilities and obligations for CIIOs to undertake, supportive measures for protection authorities to adopt and the legal liability for violation. Significantly, the CII Security Regulation put forward several factors to consider in identifying CII, namely:

- the importance of the network facility and information system;
- the degree of harm that might be caused in the event of destruction, loss of function or leak of data; and
- the impact on the relevant industries and sectors.

Additionally, the Regulation specifies that industry regulators are charged with the responsibility to identify the CII, and notify the operator thereof about the identification result.

Because CIIOs are subject to heightened compliance obligations, some of which may affect how they should interact with other companies (eg, procurement), companies should be mindful of any notices from relevant regulators and the CIIO status of the business clients.

Industry-Specific Regulations

Cybersecurity regulations are moving toward a sectoral model, where industry regulators are implementing the laws with industry-specific issues.

On 23 January 2022, the financial regulators issued a five-year plan to advance the standardisation of financial sectors. The plan, by recognising the cybersecurity and data risks brought by the digitalisation of financial services, aims to improve network security standards in the financial sector, such as financial CII protection standard, financial network security assessment, etc, so that financial service providers are well equipped against cybersecurity threats. In particular, the plan contemplates financial information technology outsourcing evaluation, financial data classification and commercial cypher codes standards.

The Ministry of Industry and Information Technology (MIIT) issued the Administrative Provisions on Security Vulnerabilities of Network Product on 12 July 2021. Network product suppliers, network operators and vulnerability publication platforms are required to set up a communication channel to receive reports of network products' security vulnerability, and keep the log of the received security vulnerability for at least six months. Additionally, network product suppliers are required to report identified vulnerability information to the National Vulnerability Database within two days.

Furthermore, the MIIT has twice sought public comments for the Data Security Management Measures of Industry and Information Technology Sector – in September 2021 and February 2022 – indicating MIIT's commitment to establishing detailed data security rules. The Measures first divides data into three categories: normal data, important data and core data, then provides the identification criteria, based on the degree of impact on national security, public interests and private interests. The Measures also offer detailed requirements for each category of data through every step of data processing activities. Similar to the draft Data Security Regulation, the Measures require companies to file the important data identification result with the regulators.

Switching to the automotive sector, the CAC and four other regulators, including the Ministry of Transportation, issued the Automotive Data Security Management Measures in August 2021. For the first time, the Measures provide a clear definition of important data, including more than 100,000 individuals' personal information and geographic information of sensitive areas such as government buildings. The Measures also require automotive data processors to file an annual data security management report with the competent authorities, specifying the types, volume, purposes and necessity of automotive data processing activities, as well as the implemented protective measures.

Conclusion

Starting from the CSL, security obligations are determined based on different legally prescribed roles, and potential impact on national security, public interests and private interests, such as that CIIOs are subject to higher security protection obligations compared to network operators. Although the overall enforcement actions are not as frequent as those in other fields, it demonstrates that regulators are taking a prudent approach in regulating cybersecurity. The cybersecurity review, MLPS and finalised (as well as proposed) filing requirements all provide regulators with effective regulatory tools and serve as bridges between cybersecurity and data security.

As such, the offshore model adopted by MNCs is likely to face more compliance burdens and may attract regulatory scrutiny. Therefore, in addition to data localisation, the possibility of network localisation should also be evaluated.

King & Wood Mallesons is an international law firm headquartered in Asia with a global network of 27 international offices. KWM's cybersecurity team is one of the first legal service teams to provide professional services concerning cybersecurity and data compliance in China; it consists of more than ten lawyers with solid interdisciplinary backgrounds, mainly located in Beijing, while further specialisms are found within KWM's global network. The team has expertise in assisting clients in responding to cybersecurity inspections and network emergencies, the establishment of network information compliance systems, self-assessment, internal training on cybersecurity and data compliance, and other related matters. Recently, KWM advised a renowned short-term lodging platform on compliance with the multi-level protection of cybersecurity, during which KWM provided elaborative analysis on the current graded protection obligations and further comparatively analysed the newly proposed mechanism and the existing one, thereby enabling it to offer practical advice to the client.

AUTHORS

Susan Ning is a senior partner and the head of KWM's regulatory group. She is one of the pioneers engaged in cybersecurity and data compliance practice, with publications in a number of journals, such as the "Journal of Cyber Affairs". Her publications include "Big Data: Success Comes Down to Solid Compliance" and "No Data, No Internet of Vehicles". Susan's practice areas cover self-assessment of network security, responding to network security checks, data compliance training, etc. She has assisted companies in sectors such as IT, transportation and finance in dealing with network security and data compliance issues.

Han Wu is a partner of KWM's regulatory group. He excels in providing cybersecurity and data compliance advice to multinationals' Chinese branches and in establishing network security and data compliance systems for Chinese enterprises operating abroad. In the areas of cybersecurity and data compliance, Han provides legal services, including assisting clients in establishing a cybersecurity compliance system, self-investigation on cybersecurity, network security investigations, cybersecurity incidents, data fusion and identification of data assets. Han has provided legal services on cybersecurity and data compliance to companies in multiple industries. The projects in which he has participated encompass the financial payments, consumer electronics, internet advertising and healthcare industries.

Contributed by: *Susan Ning and Han Wu,* ***King & Wood Mallesons***

King & Wood Mallesons

18th Floor, East Tower
World Financial Center
1 Dongsanhuan Zhonglu
Chaoyang District
Beijing
100020, PRC

Tel: +86 10 5878 5588
Fax: +86 10 5878 5566
Email: kwm@cn.kwm.com
Web: www.kwm.com

Chambers Guides to the Legal Profession

Chambers Directories are research-based, assessing law firms and individuals through thousands of interviews with clients and lawyers. The guides are objective and independent.

practiceguides.chambers.com