Chambers

GLOBAL PRACTICE GUIDE

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

Data Protection & Privacy

China: Trends & Developments

Global Law Office

chambers.com

2020

Trends and Developments

Contributed by:
Maggie Meng, Vincent Wang and Jerry Liu
***Global Law Office** see p.6*

Chinese legislation regarding data compliance and personal information protection has three defining characteristics.

Comprehensiveness – it covers both network operation security and cyber information security, while providing data protection and safeguarding citizens' lawful rights via various instruments.

Creativeness – taking China's fundamental realities into consideration, the legislative bodies adopted the concepts of the Multi-Level Protection Scheme (MLPS) and Critical Information Infrastructure (CII), which collectively build a Chinese-style data protection regime.

Hierarchy – from a general overview to specified provisions, the legislative bodies have published laws, administrative regulations, departmental rules, and national standards that jointly regulate the obligations of data controllers as well as data subjects' lawful rights and which constitute the current systematic legal framework.

With the aforementioned characteristics very much in evidence, 2019 witnessed a number of changes to both data security and privacy protection regulatory mechanisms in China. These changes improved regulatory efficiency, yet left room for further regulatory enhancement in the future. While several regulations and national standards were promulgated or released and became effective, some other draft administrative regulations and national standards were only circulated for public comment and have not yet come into force. Chinese governmental authorities are stepping up the pace in data compliance and personal information protection, shifting their focus from legislation to enforcement.

We predict that China will see two drafts of specific laws in this area in 2020, the Personal Information Protection Law of the People's Republic of China (Personal Information Protection Law) and the Data Security Law of the People's Republic of China (Data Security Law). These two laws, together with the Cybersecurity Law of the People's Republic of China (Cybersecurity Law), will constitute the cornerstones both of China's legislative system and its enforcement programme in this area. The year 2020 is very likely to be another landmark one for data compliance and personal information protection in China.

This article analyses the past and forecasts the future. The general suggestion is that businesses should at least pay close attention to these new developments and prepare any adjustments that will need to be made in the new era. We hope that this article is helpful in providing guidance to foreign and domestic businesses that have compliance needs in this area within China.

Changes and Developments in 2019

In 2019, rules regarding the security of data and personal information were dispersed in laws and regulations. Based on the classification of regulated subjects (the normal network operators and Critical Information Infrastructure Operators - CIIO) and the categories of protected data (personal information, important data, CII, and other data), several important draft regulations and national standards were circulated for public comment. The regulatory authorities are taking stricter enforcement measures, which shows the government's willingness to enforce high standards in data compliance and personal information protection.

Old laws revised

Firstly, 2019 witnessed three draft revisions to the national standard Information Security Technology – Personal Information Security Specification, which became effective on 1 May 2018. This national standard provides the measures and mechanism that companies are recommended to use in order to ensure personal information protection compliance. For the purpose of addressing the latest developments in information technology, three drafts of this standard were released separately in February, June, and October 2019. These drafts presented more practical guidance for regulation, including but not limited to, the techniques of Software Development Kit (SDK), personalised display for individuals, and rules regulating the collection and use of data.

Secondly, the new national standards of China's MLPS for networks became effective on 1 December 2019, including: (i) GB/T 22239-2019 Information Security Technology – Baseline for Multi-level Protection of Cyber Security; (ii) GB/T 25070-2019 Information Security Technology – Technical Requirements of Security Design for Multi-level Protection of Cyber Security; and (iii) GB/T 28448-2019 Information Security Technology – Evaluation Requirement for Multi-level Protection of Cyber Security (collectively New MLPS National Standards). The New MLPS National Standards overall maintained five levels for security protection specified in the MLPS. In addition, recognising the fact that emerging technologies (eg, cloud

computing and AI) create new cybersecurity concerns, the New MLPS National Standards address these new concerns by setting forth special requirements. In the transition from "Multi-level protection over information security" (commonly referred to as MLPS 1.0) to Multi-level protection over cybersecurity (commonly referred to as MLPS 2.0), the New MLPS National Standards present the recommended technical best practice under MLPS 2.0.

New laws (or their drafts) promulgated

The Cyberspace Administration of the People's Republic of China (CAC) released two eye-catching regulations in 2019, the Administrative Measures on Data Security (draft for public comments), in May, and the Measures on Assessing the Security of Cross-border Transfer of Personal Information (draft for public comments), in June. Compared to the Information Security Technology – Guidelines on Assessing the Security of Cross-border Data Transfer (draft for public comments) and the Measures on Assessing the Security of Cross-border Transfer of Personal Information and Important Data (draft for public comments) circulated in 2017 from the China National Information Technology Standardisation Committee, the new draft regulations indicate that the agency is changing its legislative and regulatory methodology to differentiate "personal information data" and "important data".

On 1 October 2019, the Provisions on the Cyber Protection of Children's Personal Information took effect. This is the first regulation focusing on the protection of children's personal information. While specifying detailed requirements for the protection of children's personal information, it prohibits any organisation or individual from producing, releasing, or disseminating information, without the consent of the children's guardians, which may infringe those children's personal information security. It also sets forth the regulatory powers of the CAC and its local counterparts, and the other related governmental authorities.

Lastly, 2019 also saw a set of enforcement actions taken by the CAC, the Ministry of Information Industry Technology, the Ministry of Public Security, and the State Administration for Market Regulation (collectively, the Four Ministries) against app operators whose apps had illegally collected and used personal information. The Four Ministries established the special work group on app governance and jointly published the Announcement on Special Governance of the Illegal Collection and Use of Personal Information by Apps, specifying, among others, the app operators' security obligations and regulatory penalties. In these regulatory actions, the Four Ministries investigated millions of apps and released official warnings or even ordered app store operators to take certain apps offline due to their non-compliant behaviours in collecting and using personal information. In order to address the compliance issues identified in the investigation, the Four Ministries, together with the special work group on app governance, enacted new regulatory rules such as: (i) the Self-evaluation Guidelines on Avoiding Collecting and Using Personal Information Illegally; (ii) the Information Security Technology – Basic Specification on Collecting and Using Personal Information by Mobile Internet Applications; and (iii) the Measures on Determining Illegal Collection and Use of Personal Information by apps. The above rules not only provide guidance on the substance of the privacy guidance documents published to the general public, but also shed light on the compliance faults affecting privacy by design and by default of apps, which secure users' right to know and right to choose. For example, the app's privacy policies are required to exhaustively list all the personal information that it will collect and to be easily accessible by users. Where apps collect personal information without limitation and damage user privacy, these regulatory rules and law enforcement actions will step in and investigate.

Trends in 2020

As of the date of this article, China has over 40 laws and 230 regulations and legislative documents covering the areas of data compliance and personal information protection. This creates difficulties in maintaining consistent law enforcement in practice. Regulatory enforcement may be duplicative or miss a loophole; and the discretion exercised in enforcement over the same issue may be inconsistent, which will result in inefficiency in law enforcement and confusion for businesses.

However, the complexity and confusion in the legal system are changing and improving. According to an official news report, two laws concerning data and privacy are listed in the legislation plan of 2020: the Personal Information Protection Law and the Data Security Law. Once promulgated, they will contribute to the building of a comprehensive and complete legal system of data compliance and personal information protection and guide the relevant law enforcement actions in a more unified, co-ordinated, and efficient manner. In brief, we expect the following changes in the areas of data compliance and personal information protection in 2020.

More legal support on specific issues

As mentioned above, national-level legislation on privacy compliance and personal information protection is missing in the current legal system. Relevant national-level legislation can only be found in some general provisions of the Cybersecurity Law and the Consumer Rights Protection Law, which is inadequate for individuals to protect their privacy and insufficient for law enforcement.

With the release of the above two laws, we expect that the government may simultaneously release certain technical regulations and standards, aiming to substantiate the compliance obligation of businesses and to provide practical guidance on the fulfilment of those obligations while facilitating the public's ability to safeguard the rights of personal information protection.

Multiple dimensions in regulation

The coming year may bring legislation regarding different cybersecurity subjects. Taking CIIO as an example, pursuant to the Cybersecurity Law, CIIO must undertake stricter obligations than other non-CIIO organisations. There are a set of draft regulations and national standards regarding CIIO. If released in 2020, these would provide more specific guidance to define a CIIO and its obligations.

Additionally, the Information Security Technology – Personal Information Security Specification, which had three draft revisions in 2019, is likely to be finalised. The new national standards would regulate data compliance comprehensively throughout the data's whole life cycle: from its collection, use, storage and transmission, to its deletion. Once issued, it will serve as a detailed standard to provide enforcement guidance for the forthcoming Personal Information Protection Law.

Furthermore, with the regulation of cross-border data transfer remaining unsettled, the development of draft legislations concerning cross-border data transfer in 2020 is an important aspect for businesses at home and abroad. Such draft regulations include Measures on Assessing the Security of Cross-border Transfer of the Personal Information and Important Data (draft for public comments), Information Security Technology – Guidelines on Assessing the Security of Cross-border Data Transfer (draft for public comments) and Measures on Assessing the Security of Cross-border Transfer of Personal Information (draft for public comments).

Lastly, measures and national standards on data processing and internal compliance operations are still in draft status – eg, Information Security Technology – Guidelines on Deidentification of Personal Information (draft for public comments), Information Security Technology – Guidelines on Personal Information Security Assessment (draft for public comments) and Information Security Technology – Guidelines on Informed Consents of Personal Information (draft for public comments). We may see these draft standards put into practice after finalisation in 2020.

Construction of the data law

We expect the future legal mechanism of data protection to be based on three basic laws: the Cybersecurity Law; the forthcoming Personal Information Protection Law; and the expected Data Security Law. Each of them represents a separate dimension of cyberspace regulation.

The Cybersecurity Law regulates general security issues of cyberspace – including the construction, operation, maintenance and use of the network – and sets forth the rules regarding the operational security of critical information infrastructure and regulatory authorities' responsibilities.

The forthcoming Personal Information Protection Law will likely regulate the security issues during the life cycle of personal information, including the security obligations of data controllers and data processors and the lawful rights of data subjects. The forthcoming Data Security Law will likely regulate the security issues during the life cycle of important data and non-personal information, with an emphasis on big data, and set forth obligations for data controllers. The draft Administrative Measures on Data Security (draft for public comments), promulgated in 2019, is expected to be a regulation to implement the Data Security Law.

The comprehensive structuring of data legislation provides a clear roadmap for enterprises to follow and to carry out internal compliance management systematically and efficiently.

Stricter regulation in key industries

In the general background of more strict regulations, the competent authority for each industry, especially key industries, is expected to develop detailed rules on the implementation and enforcement of data compliance and personal information protection as well as the penalties. Such detailed rules will likely be enacted pursuant to the above-referenced basic laws and tailored to fit specific industries. The key industries in this paragraph include: (i) under the Cybersecurity Law, the seven important industries that have critical information infrastructures, which are public communication and information services, energy, transportation, water conservancy, finance, public services, and e-government; and (ii) other industries that have a critical influence on basic livelihood and public security.

Challenges for Businesses

The coming year will be a challenging one as regards compliance for businesses at home and abroad. As China is improving its legislation regarding cybersecurity and personal information protection, the compliance requirements for enterprises are becoming more challenging. Some of the major challenges are set out below.

Management requirements for construction, operation, maintenance and use of an enterprise's network

The forthcoming Data Security Law (draft for comments), Administrative Measures on Data Security, and other relevant

regulations and standards for critical information infrastructure are expected to be promulgated in 2020. These laws and regulations will set forth detailed cybersecurity obligations for network operators, especially those classified as CIIOs. Enterprises subject to those laws and regulations should internally review their network architecture in accordance with the available regulations and specifications, in order to prepare for the forthcoming compliance work.

Cross-border transfer of data

China does not have a unified mandatory requirement for data localisation; instead, based on the data categories and operators' different roles, it has promulgated regulations separately. The Cybersecurity Law requires CIIOs to locally store the personal information and important data collected and produced during their operation within China, with certain exceptions. The Administrative Regulations on Credit Investigation Industry requires, generally, that credit investigation information should be stored within China. As a rule, personal information relevant to national secrets and state affairs, national health, maps, online car-hailing services, and so on are prohibited from being transferred abroad. Measures on Evaluating the Security of Cross-border Transfer of the Personal Information and Important Data (draft for public comments) expands the restricted subjects, CIIOs under the Cybersecurity Law, to "network operators" more broadly and requires them to obtain the consent of the personal information data subject and not to endanger national security and societal interests, nor to transfer the data cross-border without the approval of the designated authorities.

Pursuant to the drafts of the Administrative Measures on Data Security and the Measures on Security Assessment for Cross-border Transfer of Personal Information promulgated in 2019, the cross-border transfer of important data and personal information requires not only the approval of competent government agencies but also the prior risk assessment of such cross-border security by the network operator. In addition, network operators are required to enter into contracts with the recipients of personal information before the cross-border transfer, and such contracts should disclose the recipient and its security obligations, the purpose of transfer, etc. Furthermore, network operators are obligated to annually report the cross-border transfer of personal information within the preceding year to the designated government authority, and to keep a record of the transfer for at least five years following such transfer.

Whether the above requirements will evolve in 2020, and to what extent such requirements can be implemented, are going to profoundly affect the data compliance work of businesses. Businesses should keep one eye on developments in this area in 2020.

Regulatory landscape of the government

The core value of data compliance and personal information protection is to protect the lawful rights of data subjects and to maintain cybersecurity. In 2019, violations were found in tens of thousands of apps during investigations jointly carried out by the Four Ministries. The businesses operating the apps that failed to meet the compliance requirements were subject to administrative penalties (such as taking the app offline), administrative questioning, fines, and even criminal investigations in some extreme cases. In late 2019, several companies working in big data analysis for financial credit ratings were investigated for their illegal collection and sale of personal information using web crawler technology.

Each business should carefully review its own data compliance issues and adjust its risk control policy in time to comply with this new trend in law so as not to have its reputation impaired or incur other losses. Multinational companies should constantly review their global policies regarding data compliance based on worldwide legislative changes and particularly focus on their policy implementation in China while being mindful to process their data and personal information in accordance with the development of relevant regulations and standards.

*****

In conclusion, in 2019, the competent authorities' administration and management focused mainly on regulating the illegal collection and misappropriation of personal information, while their administrative surveillance is moderate on the storage and cross-border transfer of personal information. The forthcoming Personal Information Protection Law and Data Security Law, if enacted in 2020, are expected to greatly strengthen their regulatory powers and increase penalties during the data life cycle. Businesses, both domestic and international, should proactively review their current data compliance policies and compare their compliance measures with the requirements set forth in the drafts of the foregoing laws. By doing so, they can have sufficient time to fill in the potential compliance loopholes and better prepare for the forthcoming legislative updates in China's data compliance and personal information protection regime.

Global Law Office dates back to 1984, when it became the first law firm in the People's Republic of China to take an international perspective on business, fully embracing the outside world. With more than 400 lawyers practising in the Beijing, Shanghai and Shenzhen offices, it is now also known as one of the leading Chinese law firms and continues to set the pace as one of the PRC's most innovative and progressive legal practitioners. The firm has rich experience in handling various complex inbound and outbound matters. Team members have a deep understanding of corporate operations and requirements in this field, providing cutting-edge services to clients from industries which include technology, communications and media, banking and financial services, life sciences and pharmaceuticals, education, electronics and manufacturing. Services include compliance and regulatory, data mapping and audits, data security and accessing subjects' rights, data management and investigations, global data transferring, etc.

Authors

Maggie Meng has been the general counsel and DPO at different companies, and now leads a team dedicated to the full range of professional data compliance legal services, helping clients build their domestic and international data compliance systems. Her current clients include multinational companies, notable internet giants, unicorn companies, commercial banks, fintech, IoT and pharmaceutical companies, etc. Maggie has also successfully provided data compliance/governance courses for many institutions and government authorities, such as the International Association of Privacy Professionals (IAPP) and the Office of Tianjin Cyberspace Affairs Commission.

Vincent Wang is a partner of Global Law Office based in Shanghai. His practice areas cover new and emerging technologies (such as AI, blockchain, IoT, e-mobility and cloud computing), business operations, M&A, complex transactions, intellectual property, industrial regulation and compliance, cybersecurity, data regulation and dispute resolution. His clients, both domestic and multinational, come from a wide range of industries, including telecommunication, E-commerce, electronic payments, internet-related businesses, high-tech manufacturing and engineering, automotive, media and entertainment, food and beverage, and agriculture and farming.

Jerry Liu is a partner of Global Law Office based in Shanghai. He has extensive experience in the areas of data protection and privacy, investment, M&A, PE/VC, compliance/anti-corruption, and dispute resolution. Jerry provides the aforementioned legal services to many Fortune 500 multinational companies as well as Chinese companies. His clients cover a wide range of industries, including automobile, insurance, energy, pharmaceuticals, retail and TMT.

Global Law Office

15&20/F Tower 1, China Central Place
No 81 Jianguo Road, Chaoyang District
Beijing 100025
China

Tel: +86 10 6584 6688
Fax: +86 10 6584 6666
Email: global@glo.com.cn
Web: www.glo.com.cn