

Chambers



GLOBAL PRACTICE GUIDES

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

Data Protection & Privacy

China: Trends & Developments

Vincent Wang

Global Law Office

practiceguides.chambers.com

2021

Trends and Developments

Contributed by:

Vincent Wang

Global Law Office see p.7

The year 2020 established three milestones in China's personal information protection and data security legislation: the Civil Code of the PRC (Civil Code), the draft Personal Information Protection Law of the PRC, and the draft Data Security Law of the PRC. The Civil Code has laid the civil law foundation for personal information protection. The Personal Information Protection Law and the Data Security Law, once they have become effective, will be the fundamental laws covering, respectively, personal information protection and data security.

Other than those three milestones, 2020 also saw a lot of regulatory mechanism changes happen in China's personal information protection and data security space. In addition, China's digital economy strategies took a leap towards implementation in 2020. Several national plans for implementation have been issued to accelerate the development of a data-based digital economy. We foresee that more enforcement measures and judicial interpretations will be issued to protect personal information and data, and, at the same time, promote industrial and commercial data exchange, integration, and usage.

In this article, we will summarise the developments in China in all the above fields in the past year. In 2020, China continued tightening regulations to protect personal data, took great efforts to finalise its implementation strategy on data protection and made meaningful attempts to incubate a sharing and exchange mechanism for industrial and commercial data. We expect that 2021 will become a particularly important milestone for China to reveal and implement its complete data strategy domestically and internationally. Chinese and foreign businesses may want to pay close attention to any data-related developments for the incoming opportunities and challenges, both in and from China.

Personal Information Protection in 2020

Chinese lawmakers have released several important laws and draft legislations in 2020 regarding personal information protection and data security.

The most significant development in this year is that the long-awaited foundations of a unified data legal framework have been laid in China, in its Civil Code.

Changes in laws

Civil Code

Civil Code was released in 2020 and become effective on 1 January 2021. It is the root of all laws of personal information protection, as it declares that personal information should be protected under the civil law and, furthermore, it ended the long debate about the difference between personal information and privacy. The Civil Code has defined both privacy and personal information and differentiated between the right to privacy and the right to personal information. It confirmed that personal information and privacy are parallel legal concepts, and neither is inclusive of the other.

Personal Information Protection Law

Chinese legislators also released in 2020 the draft Personal Information Protection Law (the Draft Law) for public comments. The Draft Law aims at establishing a dedicated foundation for personal information protection and attempts to address most of the hotly debated issues, such as the legitimacy of facial recognition technology, the proper exploitation of the individual tracking data collected for the control of the COVID-19 pandemic. It also mirrors the trends under the General Data Protection Regulation (GDPR) of the EU and makes good faith efforts to bring Chinese personal information protection mechanisms in line with current international mainstream standards.

The Draft Law defines personal information as information relating to an identified or identifiable natural person, as recorded in electronic or other forms. This definition of personal information is wider than the one stipulated in the Civil Code and the Cybersecurity Law of the PRC (with effect from 1 June 2017), where personal information only refers to the information recorded in electronic or other forms that can identify, independently or in conjunction with other information, specific individuals. The definition under the Draft Law focuses more on the relevance of information to individuals, rather than the ability of information to identify individuals. The legislature has not explained why there is an apparent deviation in the definition. However, the wording of the definition under the Draft Law almost literally follows the definition of "personal data" under the GDPR. It remains to be seen whether further clarifications or amendments will be provided in future revisions of the Draft Law.

In addition, the Draft Law has incorporated several mechanisms similar to those stipulated in the GDPR, including the:

- extra-territorial applicability of the Draft Law;
- diversified legal basis of data processing;
- comprehensive rights of personal information subjects throughout the full life cycle of data processing;
- liabilities of joint processors;
- automated decision-making; and
- prohibitive administrative fines for personal information processing violations.

Like many other pieces of Chinese legislation, the Draft Law also included the “Chinese approaches” to regulate the illegal processing and transfer of personal information, such as the adoption of a “black-list”. Foreign organisations and individuals on the blacklist are forbidden to receive personal information from the PRC.

The Draft Law is surprisingly comprehensive and well-considered. However, with some key questions still unanswered, further substantive efforts may need to be exerted before the draft can be finalised, which may be expected at some point in 2021.

Protection of minors

The protection of the personal information of minors (those under the age of 18) is a hot topic. In the modified Law of the PRC on Protecting Minors, the newly added Chapter V on Online Protection attempted to address concerns around this issue in the information age, such as cyberbullying or other harms to minors by abuse of their personal information over the internet.

The modified law has stipulated that the processing of a minor’s personal information should be subject to the principle of lawfulness, legitimacy and necessity. The processing of personal information of a minor under the age of 14 should be further subject to the consent of the minor’s parents or guardian.

Recommended national guidelines

China has also released a revised version of the Information Security Technology – Personal Information Security Specification in 2020 (Personal Information Security Specification). It is a recommended national standard of the PRC and a major practice reference for personal information protection in China. The revised Personal Information Security Specification came into force on 1 January 2021.

Compared with the previous version that was released in 2017, the new Personal Information Security Specification has made adjustments to address the latest issues and emerging technologies related to personal information protection, such as user

profiling and automated decisions, sensitive personal information, third party software development kits (SDKs), application programming interfaces, etc. The new Personal Information Security Specification aims at helping companies increase more clarity and efficiency in the data compliance.

Last but not least, China released a new national standard for personal information protection, the Information Security Technology – Guidance for Personal Information Security Impact Assessment (PIA Guidance) in 2020. The PIA Guidance is of great value in guiding the personal information security impact assessments made by companies, as there are no detailed requirements for such assessments provided in the existing laws.

Judicial procedures against infringements of personal information

Personal information disputes – a new type of lawsuit

The Supreme Court of China issued several judicial interpretations regarding personal information disputes at the end of 2020 to assist with personal information protection upon the coming into effect of the Civil Code. A notable change included among these judicial interpretations is that infringement of personal information will be newly categorised as an independent type of lawsuit. Such a change is in response to an independent legal basis of personal information protection being established in the Civil Code. Prior to the Civil Code, infringements of personal information were tried usually under personality rights lawsuits regarding privacy, contract law, or competition law.

The first case regarding facial recognition technology

There were also several court decisions against harms to personal information in 2020. Perhaps the most widely noted case of 2020 was one in which the plaintiff, a law professor visiting a zoo, sued the zoo for the attempt to compel collection of his facial recognition information.

Due to the lack of a clear legal basis under the law, the court avoided analysing the collection of facial information or the legitimacy or illegitimacy of facial recognition technology. Instead, the court moved to analyse, under the laws of contract and consumer protection, whether the zoo had breached its contractual obligations in the collection of the plaintiff’s biometric information.

According to the court’s decision, the zoo should delete the plaintiff’s biometric information, because the collection of such personal information is unnecessary for the performance of the consumer contract between the zoo and the plaintiff. The case was tried by the court as a consumer protection dispute. The attempted collection of the plaintiff’s facial information was analysed as an issue of whether the zoo respected the consumer

CHINA TRENDS AND DEVELOPMENTS

Contributed by: Vincent Wang, Global Law Office

plaintiff's right to information rather than whether attempted collection of such facial information is improper under the law.

Personal information infringement in criminal cases

Infringements of personal information can be prosecuted through public interest lawsuits in criminal cases. Such lawsuits have been brought up by several local prosecutor's offices in 2020. There is also a trend for procuratorates becoming increasingly active in pursuing public interest cases in civil proceedings of personal information protection. We will see more of such cases in 2021.

Hot topics in personal information protection

App regulations

In 2020, the Ministry of Information Industry Technology (MIIT) continued administrative investigations against non-compliant apps. The MIIT investigated over 520,000 apps in 2020, among which 1,571 were cited as being non-compliant due to their personal information processing. The non-compliant apps were publicly warned or ordered to be taken down by the MIIT.

Non-compliant collecting and processing of data spotted in the investigation has been addressed by a set of new regulatory documents and guidelines released by the MIIT, regulatory authorities and industrial associations. The regulatory documents and guidelines provide detailed specification and compliance guidance to help app operators fulfil their regulatory obligations. In addition, the administrative investigations against non-compliant apps have indicated that the transparency of using third-party SDKs and policies relating to account deletion have become new focuses of app regulation.

Personal information protection during the COVID-19 pandemic

Personal information protection has been escalated because of the COVID-19 case-tracking mechanisms used in 2020. Several administrative rules and national standards over personal information protection have been released in the context of the pandemic. Those rules and standards provide specific guidance to app operators about personal information collection and processing for the purposes of COVID-19 case tracking.

Individuals who post or forward COVID-19-related news or pictures disclosing individual personal information on social media may be punished with an administrative penalty. The police have investigated and imposed fines in several personal information infringement cases in 2020. Those cases show that personal information protection in China is not only enforced in commercial scenarios, but also in the administrative context.

Cross-border transfer

The draft Personal Information Protection Law attempts to establish a new framework for personal information cross-border transfers by satisfying businesses' needs, aligning Chinese standards with GDPR practice and addressing security concerns.

Under this framework, cross-border data transfer will be lawful after satisfying one of the following three requirements:

- conducting a security assessment organised by competent agencies under the Cyberspace Administration of China;
- obtaining personal information protection certification from government-designated professional organisations; and
- entering into contracts with the transferee to specify both parties' rights and obligations with regard to personal information protection requirements.

Separate consent from each personal information subject is always required for the cross-border transfer of personal information, regardless of which of the above requirements is the legal basis relied upon. Such rules are stricter than the rules of cross-border data transfer in the EU GDPR.

Data Security

The move towards a data economy is guiding the legislation on data security. A significant development on data security in 2020 was the release of the draft Data Security Law. The draft Data Security Law aims at a balance between data protection for security and data sharing for the economy. Practice guidelines released in 2020 are sector-focused, such as the security guidelines on industrial data, on health and medical data, etc. Furthermore, several implementation plans have been issued at national level this year to accelerate data sharing and exchange for the development of the digital economy. Industrial data will be the next focus in 2021.

Changes in law

Data Security Law

The draft Data Security Law of the PRC (Data Security Law) has been released for public comments in 2020. It is the first draft law focusing on data security in China. The Data Security Law establishes a general legal framework protecting the safety and security of data of any kind recorded in electronic or other forms.

However, the Data Security Law also pays attention to balancing the requirements of data security and data sharing for digital economy. It encourages data sharing and data trading to develop the economy, but it also outlines a series of data security obligations for data processors, especially the processor of important data and the data trade broker. For example, the processor

of important data should take appropriate organisational and technical measures, including incident reports and regular risk assessments of data processing, to ensure the security of important data. Data trade brokers are obliged to review and record information about the data purchaser and the data seller as well as transaction information, including the source of the data in question.

Practice guidelines relating to data security

Practical guidelines for data security

Several guidelines for data security relating to specific industries have been released in 2020, including: (i) the Guidance on Establishing Data Security Specifications in the Telecommunications Industry and the Internet, (ii) the Guidance on Establishing Data Security Specifications for Online Data, (iii) the Pilot Guidance on the Classification of Industrial Data, (iv) Financial Data Security – Guidance on Data Security Classification and (v) Information Security Technology – Guidance on Data Security of Health and Medical Data;

In addition, there were several draft guidelines released in 2020, such as (i) the draft Guidance on Data Security in Online Car-Hailing Services, (ii) the draft Information Security Technology – Guidance on Big Data Security in Telecommunications, and (iii) the draft Information Security Technology – Security of Online Data Processing.

National standards and administrative guidelines remain the major practical compliance guidance for data processors in China because the legal framework of data security provides high level principles with very general clarifications. In order to be practical, the national standards and administrative guidelines are mostly sector-focused with more specific guidance in relation technical and operational aspects.

Practical guidelines of cybersecurity

Data processors should also pay attention to the practice guidelines for cybersecurity as well ensuring the security of information systems where data is stored and processed.

Authorities released several national standards for the cybersecurity classification of information systems and critical information infrastructure in 2020. Among those national standards, the revised Information Security Technology – Classification Guide for Multi-Layer Protection of Cybersecurity (Classification Guide) was released in 2020. The revised Classification Guide has added cybersecurity classification requirements for cloud computing systems, the internet of things (IoT) systems, and industrial control systems.

However, there have been no substantial upgrades to cybersecurity requirements and standards in 2020.

Data Economy

Implementation of data economy strategies

The year 2020 was one of data strategies for China. A lot of incentivising plans and rules were released to encourage building a solid foundation for the data economy.

In August 2020, the Chinese government issued the general plan and the pilot implementation plan to further develop the innovative service trade. According to those plans, data economy and data trading are critical parts of the future Chinese economy. Key implementation tasks include, but are not limited to, building data exchange platforms, and establishing the legal framework of data exchange.

Pilot free-trade zones in Beijing, Shanghai, Hunan, Anhui, Hainan, and the Shenzhen Special Economic Zone are expected to be the pioneers and to build data trading systems and test new rules and mechanisms of data trading and transfer. Beijing and Shanghai moved ahead of others to investigate and study the practical implementation of international data exchange in 2020.

Industrial internet data

The State Council of the PRC issued the Industrial Internet Innovation and Development Action Plan in January 2021, which states that the years of 2021–2023 will be the years of the industrial internet.

Several guidelines and rules regarding industrial data were released by the MIIT in 2020, including (i) the Pilot Guidance on Industrial Data Classification, (ii) the Development Guide on Industrial Big Data and (iii) the Measures for the Administration of the Industrial Internet. Exchange platforms and the rules of industrial data are expected to be established.

Trends and Developments in 2021

The year 2020 laid a good foundation for the rationalisation of a comprehensive and complete legal system for personal information protection and data security, and for guiding law enforcement actions in those areas in a more unified, co-ordinated, and efficient manner. Some of the way in which 2021 will likely witness developments building on this are set out below.

More legal basis and practical guidance

It is expected that Chinese legislators will continue polishing the draft Personal Information Protection Law and the draft Data Security Law in 2021. More clarification on key terms and the ensuring that the drafts are consistent with existing laws are both likely. They are expected to be finalised and officially released in 2021.

CHINA TRENDS AND DEVELOPMENTS

Contributed by: Vincent Wang, Global Law Office

It is also expected that the government may release, in advance or in parallel with those new laws, certain technical regulations and standards to substantiate the compliance obligation of businesses and to provide practical guidance for businesses to facilitate their compliance needs.

More data usage rules

The data economy will continue to be the focus of data security in 2021.

We also expect that the legal framework of the data economy will be improved through the passing of national legislation in 2021. Following the Personal Information Protection Law and the Data Security Law, more implementation rules and standards of data transfer are expected to be released in 2021.

In addition, more specific rules or drafts legislations may be issued at the local governmental level to facilitate the use of data, in particular the integration and transfer of industrial and commercial data, as data-exchange centres are expected to be established in several free-trade zones in various cities, as mentioned above.

More civil disputes

The Supreme Court has declared personal information disputes to be a new form of civil dispute, The Supreme Procuratorate has released the policy to support public interest cases involving personal information. With more and more laws and rules to be put in place, it is also anticipated that the courts will see more personal information protection cases. More judicial interpretations in trials of civil disputes involving personal information protection will likely be released to guide these trials and set clearer expectations for parties in such disputes.

Challenges for Businesses

General compliance

Businesses at home and abroad may find 2021 a challenging year for compliance with data protection and privacy rules. With more laws and standards being put in place, data compliance will become a more complicated and, in some areas, more delicate task.

Cross-border transfer

More specific guidance for the cross-border transfer of personal information and data will likely be seen in 2021. While a clearer understanding of the requirements is welcome, it may well become more difficult to transfer data across borders.

App regulation

In 2020, violations were found in thousands of apps during the investigations by the MIIT. Regulatory investigations by governmental authorities against apps for non-compliant data collecting and processing will continue in 2021; however, the focus of these investigations may change again.

Dispute resolution

In addition to dealing with administrative agencies' enforcement procedures and complying with the new technical and business requirements in the national standards, businesses in 2021 will find that they will also need to make efforts to avoid being sued by individual plaintiffs for personal information protection violations or the procuratorates for public interest cases.

Conclusion

A lot happened in 2020, but more will happen in 2021. In terms of personal information protection and data security development for China, 2021 may be an even more significant year than 2020. Chinese and foreign businesses may want to work more closely with their in-house legal department and outside counsel to track the changes in the law, the government administration and judicial practice. Only by doing so will they be able, not only to understand the new requirements for compliance, but also to catch all the opportunities created by the changes.

Global Law Office (GLO) dates back to the establishment of the Legal Consultant Office of the China Council for the Promotion of International Trade in 1979. This organisation renamed itself China Global Law Office in 1984 to take an international perspective on its business, fully embracing the outside world. After over 40 years of development, it has become one of the pre-eminent comprehensive law firms in the Chinese legal industry. GLO serves domestic and foreign clients

with a globalised vision, globalised team and globalised quality since its inception, allowing it to maintain a leading position in the industry in the midst of an ever-changing global economic environment. GLO lawyers are all graduates from first-tier domestic and/or international law schools, most of whom hold LL.M or higher degrees. Many partners are qualified to practice law in the USA, UK, Australia, Switzerland, New Zealand, and Hong Kong, among others.

Author



Vincent Wang is a partner at GLO. His practice areas cover a broad-spectrum of industries and he is particularly known for solving new and challenging issues in the TMT area. Examples of the industries Vincent covers include telecommunication, e-commerce, cybersecurity and data

protection, electronic payments, internet-related businesses, hi-tech manufacturing and engineering, and new and emerging technologies (such as AI, blockchain, cryptocurrency, IoT, e-mobility and cloud computing). He advises clients on market entry and complex commercial transaction strategy, structure and fulfilment, M&A deal structure, due diligence, corporate restructuring, international investment and trade policy compliance, cybersecurity and data compliance, telecoms, and e-commerce and e-payment regulation and operation, as well as dispute resolution.

Global Law Office

36th Floor, Shanghai One ICC
No. 999 Middle Huaihai Road
Xuhui District, Shanghai 200031
China

Tel: +86 21 2310 8288
Fax: +86 21 2310 8299
Email: vincentwang@glo.com.cn
Web: www.glo.com.cn

