Published on *The National Law Review* https://natlawreview.com

China Publishes National Standard for Personal Data Protection

Article By:

Todd Liao

With increased concerns regarding the safety of individual personal information, the Chinese government has clarified its existing data privacy rules regarding the collection, processing, usage, and more of personal data. Organizations operating in China should reexamine their data privacy policies in order to take into account the national standard for personal data protection, effective May 1, which provides detailed guidance for corporations to establish and maintain information governance systems.

With the development of information technology, collecting personal information has become a common business practice in Chinese commerce. But there have been many highly publicized cases of data abuse and leaks in recent years that have affected many industries, including education, healthcare, ecommerce, and telecommunications. The frequency, scale, and consequences of these incidents have made people increasingly concerned about the safety of their personal information. Businesses are also concerned about potential risk exposure in relation to customer data protection. Under these circumstances, the Chinese government decided to clarify some ambiguities in existing data privacy rules, especially in terms of the collection, processing, usage, sharing, transfer, and storage of personal data.

On August 22, 2016, the Office of the Central Leading Group for Cyberspace Affairs; the General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China (AQSIQ); and the Standardization Administration of the People's Republic of China (SAC) jointly issued Several Opinions on Strengthening National Cybersecurity Standardization Work (the Opinions). In Section II, "Strengthening the Standardization Work," the Opinions mentioned "proceeding with the promulgation of the urgently needed standard," and explicitly listed the "personal data protection standard" as a focus of the government's recent work. On December 29, 2017, the AQSIQ and the SAC published a national standard for personal information protection: the Information Security Technology—Personal Information Security Specification (the "Specification"), which will be implemented on May 1, 2018. The Specification is a result of the national standardization efforts endorsed by the Chinese government. The entities involved in its drafting included government entities, universities, research institutions, and leading internet companies such as Tencent and Alibaba. From this perspective, unlike China's existing data privacy rules, which contain mainly abstract principles, the Specification is more practical and user-friendly, providing detailed guidance for corporations in terms of the establishment and maintenance of an information

governance system.

As a “technical guideline,” the Specification is at the third, and lowest, level of national standards and is not legally binding. However, according to the Opinions, the Chinese government considers the standardization “an important component in the establishment of China’s cybersecurity system,” and the Specification is intended to play a “fundamental, normative, and guiding” role in China’s cyberspace governance. As such, given the “voice from the top” nature of the Specification, this standard is highly regarded and widely used despite the fact that it is not legally binding. The Specification has recently been cited by governmental authorities as the basis for some administrative decisions, such as a recent audit of the Cyberspace Administration of China (CAC), where Alipay was required to rectify its data collection/processing practices. Many commentators believe that the Specification sets best practices for Chinese companies for building firmwide personal data protection mechanisms, and will be used as comparison criteria when auditing companies under China’s existing data privacy rules, notably the 2017 Cybersecurity Law.

Due to the importance of the Specification in China’s data privacy policy system, as well as its potential implications for the authorities’ enforcement actions, multinational companies operating in China should pay close attention to this national standard and review their China practices accordingly to ensure compliance.

Relationship with Existing Data Privacy Laws

The Specification is said to be formulated under the umbrella of China’s existing data privacy legal regime that includes, among others, the 2017 Cybersecurity Law (CSL); the Decisions on Safeguarding Internet Safety and the Decisions on Strengthening Protection of Internet Data issued by the Standing Committee of the National People’s Congress; Amendments (V), (VII), and (IX) to China’s Criminal Law; and the Provisions on Protecting the Personal Information of Telecommunications and Internet Users. The Specification is a supplement to the existing rules, but does not go beyond the principles laid out in existing laws and regulations.

After the Specification was issued, many commented that the requirements contemplated by the Specification were stricter than those of EU counterparts. For example, the EU General Data Protection Regulation (GDPR) exempts the consent requirement for data processing in six situations. Among others, one of the commonly used nonconsensual grounds for collecting and processing personal information is “legitimate interests,” i.e., the necessity for data processing of the data controller overrides the data protection interests of the data subjects. However, a corresponding concept has not been adopted in the Specification. In a public speech, a Chinese policymaker explained that this is because the CSL explicitly requires that network operators in China obtain the data subject’s consent for collection, leaving blank on the exceptions; thus the Specification must stick to the scope of existing rules and not delve into areas on which the law is silent.

That being said, it appears that the Chinese policymaker tries to echo the international practices in the ambit of CSL. Taking the consent issue above as an example, though the Specification does not adopt the “legitimate interest” concept, the other nonconsensual grounds for data collection and processing under the Specification are largely analogous to the relevant grounds under the GDPR. To some extent, the scope of China’s nonconsensual grounds is even broader. For example, the Specification lists the necessity for product troubleshooting and news reports as grounds for data collection, which is not covered in the GDPR. And regarding “legitimate interests,” arguably the exceptions in the Specification have already covered some of the commonly seen examples of legitimate interests, including the necessity to protect the data subject’s personal property or other

significant rights and the necessity to execute a contract.

Key Definitions: Personal Information and Sensitive Personal Information

Before the issuance of the Specification, China had an existing national standard relating to personal data protection: Guideline for the Protection of Personal Information in Public and Commercial Service Information Systems (the 2013 Guideline). It seems that the Specification was promulgated on the basis of 2013 Guideline, while replacing and enriching the 2013 Guideline in many aspects. Among others, the Specification maintains the divided methodology as to general personal information and "sensitive" personal information, a concept adopted in the 2013 Guideline. As with the 2013 Guideline, different protection levels apply to these two categories (as discussed below). Notably, the definitions of general personal information and sensitive personal information are also updated in the Specification.

For personal information, the definition in the 2013 Guideline and other data privacy rules mainly refers to data that could "identify" a person, such as name and ID number. However, under the Specification, the definition of personal data is now extended to data that can be "linked" to one person. In specific, once an individual is identified through "identifiable" personal information, any other data generated by this person in his or her following activities, even that on its own cannot be used to identify a person, also constitutes personal information. This other personal data includes individual location, communications records, and individual browsing history. In an annex attached to the Specification, the policymaker lists various examples. It is noteworthy that an individual's address book, friend list, classification of friends, and hardware serial code—types of information that are not identifiable per se—are now explicitly defined as "personal information" and subject to data protection. This change indicates the policymaker's efforts to respond to the imminent society concerns over personal data safety by extending the scope of protection. Previously, many companies designed their data protection systems to only protect such identifiable personal data as ID card numbers, telephone numbers, IP addresses, etc. With the Specification in place, the policy for the first time clarifies that the data "linked" to an identified person also requires special treatment. Undoubtedly, such update places a new requirement on companies in terms of data protection compliance.

For sensitive personal information, the Specification generally takes a risk-based approach in its definition. "Sensitive personal information" is defined as "any personal information which, if lost or misused, is capable of endangering persons or property, easily harming personal reputation and mental and physical health, or leading to discriminatory treatment." On the face of the language, the policymaker defines the "sensitive" information broadly. According to the Specification, examples of "sensitive personal information" include individual identifiable information such as ID card number, IP address, financial information, healthcare information, sexual orientation, religion, unpublished criminal records, communication records, internet browsing history, GPS location, etc. In addition, the Specification enhances the protection of children as it generally provides that all information regarding children younger than 14 years old is sensitive personal information.

Application Scope

The Specification applies to the Information Controller, a new position combing the concept of the "personal information administrator" and "personal information receiver" in the 2013 Guideline. The Specification defines "Information Controller" as any organization or individual with the power to determine the purpose and method for processing personal information, including any private or public organizations. This is seemingly modeled on the "data controller" concept under the GDPR.

Consent Requirement and Notification Obligation

The Specification generally follows the basic principle set by the 2013 Guideline and the CSL that the consent of the Information Subject must be obtained before personal information is collected or processed, but puts more emphasis on the notification obligation of an Information Controller. The following information must be conveyed to the Information Subject when collecting information:

- **Personal information**: For personal information, (1) the purpose for which and the method by which personal information is collected and used, e.g., the frequency with which the information is collected, where and how long the information will be stored, and whether the information will be shared with or transferred to others; and (2) if an Information Controller indirectly collects personal information from a third party other than the Information Subject, the Information Controller must confirm with the third party that (i) the personal information is obtained from a legal source and (ii) the Information Subject has authorized the third party to disclose or transfer the personal information and the proposed use of the personal information doesn't exceed the scope agreed by the Information Subject; otherwise, the Information Controller must obtain explicit consent from the Information Subject.
- **Sensitive personal information**: The Specification for the first time distinguishes the requirements for core and ancillary functions: (1) if the information is required for an Information Controller to provide core business functions, the Information Subject must be informed of the consequence if he or she refuses to provide the information; and (2) if the information is for ancillary functions, the Information Subject must be informed of the specific ancillary function that requires the information; if the Information Subject refuses to provide the information, the Information Controller may refuse to provide such ancillary functions. However, if the Information Controller has obtained the necessary information for core business functions but does not obtain the information for ancillary functions, the Information Controller cannot cease providing the core functions due to the lack of information for ancillary functions.

In general, before an Information Subject can use an online service, a privacy policy prepared by the company’s Information Controller will be delivered to the Information Subject for consent. Previously there was no standard requirement for such policy, so the Information Controller tended to include provisions that expanded its rights to collect and process personal information. The Specification, for the first time, provides standardized content and suggested privacy policy language in order to restrict the Information Controller’s use and disclosure of the personal information collected. For example, the policy must include whether and to what extent the Information Controller can disclose the personal information to a third party; how the Information Subject can access, modify, and delete the personal information collected; and how the Information Subject can make a complaint, etc.

Rights of the Information Subject

Compared with the 2013 Guideline and the CSL, the Specification grants the Information Subject more control over the personal information collected. For example, the Information Subject has the right to (1) know what information has been collected and its purpose, and whether the information has been collected by any third party; (2) modify and delete the information provided; and (3) withdraw the consent provided.

Obligations of the Information Controller

The Specification further enhances the obligations of the Information Controller in terms of

information transfer and information security.

Under the Specification, additional obligations will arise if an Information Controller transfers personal information to a third party due to the following:

- Upon outsourcing of the personal information processing matters, the Information Controller must
    - ensure that the outsourcing arrangement is compliant with the prior consent granted by the Information Subject;
    - conduct risk assessments of the third party and ensure that the third party has sufficient capability in terms of data security;
    - supervise the third party, sign proper contracts, and conduct audits; and
    - accurately record the status of the outsourcing arrangement.
- Upon mergers, acquisitions, and reorganizations, the Information Controller must
    - ·notify the Information Subject that the Information Controller will undergo a change; and
    - ensure that the successors and assigns continue performing obligations after the change. In case of any change to the purpose of using personal information, the explicit consent from the Information Subject must be reobtained.

The Specification also requires that the Information Controller enhance measures for data security in terms of the following:

- Security incident response, which includes (1) formulating security incident response plans, (2) providing regular training at least once a year, and (3) notifying the affected Information Subject promptly.
- Control of internal access to the information collected. Specifically, the Information Controller must (1) ensure that only the relevant internal staff have access to the personal information, and (2) establish internal approval procedures for important operations on the personal information.
- Company governance. The Specification requires, among other things, that
    - the legal representative or other key management take the leading role for personal information security, including providing sufficient support to personnel and finance;
    - the Information Controller appoint key personnel or a department responsible for information protection matters;
    - the Information Controller establish a system to regularly evaluate the security risk at least once a year;
    - the Information Controller execute confidentiality agreements with the personnel processing personal information and conduct background checks on them;
    - the Information Controller provide training regarding the processing of personal information at least once a year or when there is a significant change to the privacy policy; and
    - the Information Controller conduct audits on the privacy policy, relevant company policies, and security measures.

Conclusion

The release of the Specification shows that the Chinese government takes data privacy regulations seriously. Although the Specification is not mandatory, further laws and regulations may refer to the Specification for personal information protection. Therefore, we suggest that organizations operating

in China reexamine their data privacy policies to make them compliant with the Specification. The Specification also leaves some areas blank for the development of further legislation, such as the cross-border transfer of personal information. We will continue to follow updates and will keep you posted.

National Law Review, Volume VIII, Number 72