China's Evolving Personal Information Protection Rules

CHINA REGULATION WATCH[1]
September 28, 2020

By: Greg Pilarowski | Lu Yue | Zhu Ziwei

1. Introduction

Since the issuance of the Cyber Security Law (网络安全法)[2] in November 2016, China's legislature and various government departments have released numerous laws and regulations addressing the protection of personal information, many of which we have listed for reference in Exhibit A below. Although China's rules are not consolidated in a single unified piece of legislation comparable to Europe's General Data Protection Regulation ("GDPR") or the California Consumer Privacy Act ("CCPA"), the rules do look similar in some areas, such as user rights and data minimization, but look different in others, including government approval requirements for cross-border data transfers. This article provides a summary of China's current and proposed laws and regulations that address personal information protection. We have also prepared a table in Exhibit B below, which compares China's rules with those set forth in the GDPR and the CCPA.

2. China's Legal Framework for Personal Information Protection

The rules governing China's personal information protection regime consist of laws, regulations and other standards issued by various government bodies, including laws issued by the National People's Congress (全国人民代表大会) or the Standing Committee of the National People's Congress (全国人大常务委员会), departmental regulations (部门规章) issued by national level government departments, and other normative documents (规范性文件) issued by government departments at various levels.

Three laws establish the framework for China's personal information protection regime, namely the currently-enacted Cyber Security Law, the proposed

---

[1] This China Regulation Watch is provided by Pillar Legal, P.C. (the "Firm") as a service to clients and other readers. The information contained in this publication should not be construed as legal advice, and use of this memorandum does not create an attorney - client relationship between the reader and the Firm. In addition, the information has not been updated since the date first set forth above and may be required to be updated or customized for particular facts and circumstances. This China Regulation Watch may be considered "Attorney Advertising" under applicable law. Questions regarding the matters discussed in this publication may be directed to the Firm at the following contact details: +1-925-930-3932 (San Francisco Bay Area office), +86-21-5876-0206 (Shanghai office), email: greg@pillarlegalpc.com. Firm website: www.pillarlegalpc.com.

[2] Cyber Security Law (网络安全法), issued by the Standing Committee of the National People's Congress (全国人大常务委员会) on November 7, 2016.

Data Security Law (数据安全法)[3] and the pending Personal Information Protection Law (个人信息保护法).[4] In addition, many department regulations and normative documents have been proposed or issued to support the implementation of these laws, such as the currently-enacted Provisions for the Online Protection of Children's Personal Information (儿童个人信息网络保护规定) (the "Minor Protection Rules"),[5] the proposed Measures for the Administration of Data Security (数据安全管理办法),[6] and the proposed Measures for the Security Assessment for Cross-Border Transfer of Personal Information (个人信息出境安全评估办法).[7] Various national standards also form part of China's personal information protection regime, including those issued by the National Standardization Administration (国家标准化管理委员会) and the National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会). Although these national standards are not binding rules, they do provide practical instructions for compliance with various laws and regulations. Some of the laws, department regulations, normative documents and national standards are still draft proposals, but they nonetheless reflect the direction of China's personal information protection rules and we have therefore included these proposals in this article.

In the past, the rules regarding personal information protection were dispersed among many different laws and regulations.[8] As a result, personal information protection was regulated by various administrative authorities. Since the issuance of the Cyber Security Law in November 2016, however, the Cyberspace Administration of China (网信办) ("CAC") has become the primary government department dealing with personal information protection issues.

3. Who is Required to Comply?

[3] Data Security Law (数据安全法), issued for public comment by the Standing Committee of the National People's Congress (全国人大常务委员会) on July 3, 2020.

[4] An official proposed draft of the Personal Information Protection Law (个人信息保护法) has not yet been issued for public comment. The latest unofficial draft was publicly released by Zhang Xinbao (张新宝), professor of Renmin University of China, on October 17, 2019.

[5] Provisions for the Online Protection of Children's Personal Information (儿童个人信息网络保护规定), issued by the Cyberspace Administration of China (网信办) ("CAC") on August 22, 2019.

[6] Measures for the Administration of Data Security (数据安全管理办法), issued for public comment by CAC on May 28, 2019.

[7] Measures for the Security Assessment for Cross-border Transfer of Personal Information (个人信息出境安全评估办法), issued for public comment by CAC on June 13, 2019.

[8] Prior rules addressing the protection of personal information included, for example, the Provisions on Protection of Personal Information of Telecommunications and Internet Users (电信和互联网用户个人信息保护规定), issued by the Ministry of Industry and Information Technology (工信部) ("MIIT") on July 16, 2013, Article 29 of the Consumer Rights and Interests Protection Law (消费者权益保护法), issued by the Standing Committee of the National People's Congress (全国人大常务委员会) (the "Standing Committee") on March 15, 2014, the Provisions on Security Management of Personal Information for Delivery Service Users (寄递服务用户个人信息安全管理规定), issued by State Post Bureau on March 19, 2014.

China's personal information protection regime does not include specific provisions indicating who is required to comply with the relevant rules. The general approach, however, is that any person or entity involved in the management of personal information (the "Data Operator")[9] is required to comply with the various relevant rules in order to ensure thorough protection of each personal information subject (个人信息主体)[10] (each a "User").

4. Definition of Personal Information

Under the Cyber Security Law (网络安全法), personal information is defined as all information recorded in electronic or other forms, which can be used, independently or in combination with other information, to identify a natural person's personal identity, including but not limited to the natural person's name, date of birth, identity certificate number, biological personal information, address and telephone number.[11] The Personal Information Security Specification (个人信息安全规范) also provides various examples of different categories of personal information, which we have listed in Exhibit C below.

Sensitive Personal Information

The Personal Information Security Specification (个人信息安全规范) defines the term "Sensitive Personal Information" to mean personal information that if disclosed, illegally accessed or abused, may endanger personal safety, property safety, and cause harm or discrimination to the personal reputation, physical health, or psychological well-being of the personal information subject. Personal information of individuals under the age of 14 ("Minors") and information involving the privacy of a natural person are usually regarded as Sensitive Personal Information. The Personal Information Security Specification includes various examples of Sensitive Personal Information, which we have listed in Exhibit D below.

The term Sensitive Personal Information is first used in the draft Measures for the Administration of Data Security (数据安全管理办法), which will require Data Operators to complete an official filing with the local office of the CAC if the Data

---

[9] Network operator (网络运营者) is a term widely used to describe the people or entities that are required to comply with China's personal information protection rules. This term is used in the Cyber Security Law, and refers to owners and administrators of networks as well as network providers. (See Article 76 of Cyber Security Law.) When writing about China's personal information protection rules, it is also necessary to refer to non-network operators who manage personal information in outside of an electronic network context. Therefore, we use the term "Data Operator" in this article to include both network operators and non-network operators.

[10] Personal information subject (个人信息主体) refers to any natural person identified or associated with certain personal information. See the Personal Information Security Specification (个人信息安全规范), issued by the National Standardization Administration and the State Administration for Market Regulation, which will become effective on October 1, 2020.

[11] See Article 76 of the Cyber Security Law (网络安全法).

Operator collects or processes any Sensitive Personal Information for a commercial purpose.[12] The draft also requires Data Operators to appoint a data protection officer (数据安全责任人) to be in charge of protecting Sensitive Personal Information.[13] Since the Measures for the Administration of Data Security are still in draft form, the local offices of CAC have not yet started to accept filings related to Sensitive Personal Information.

The Minor Protection Rules do not require Data Operators to complete any filings when they collect or process personal information of Minors that is deemed to be Sensitive Personal Information, but these rules do require "dedicated personnel" to be in charge of protecting any Minors' personal information that the Data Operator collects or processes.[14] The Minor Protection Rules do not provide additional details about qualification requirements or mandated responsibilities of the dedicated personnel, but they do specify that the dedicated personnel will need to comply with any requirements that apply to data protection officers under the Measures for the Administration of Data Security when those measures come into force.

Data Protection Officer

China's currently effective personal information protection rules, as opposed to proposed or draft rules, do not yet require appointment of a data protection officer. The draft Measures for the Administration of Data Security and several national standards do, however, provide some guidance about what this position will likely involve once those rules become effective. The relevant draft rules indicate that a data protection officer should have relevant management experience and data security experience. In addition, a data protection officer will participate in essential decisions on data activities and report directly to the person in charge[15] of the Data Operator.[16]

The data protection officer will also be required to:

- Organize the development of a data protection plan and supervise the implementation of such plan;
- Organize the assessment of data security risks and supervise the mitigation of those risks;

[12] See Article 15 of the Measures for the Administration of Data Security (数据安全管理办法), issued for public comment by CAC on May 28, 2019.
[13] See Article 17 of the Measures for the Administration of Data Security.
[14] See Article 8 of the Minor Protection Rules.
[15] Person in charge refers to the legal representative, or a person who performs the duties of the legal representative pursuant to the relevant laws and regulations. Companies established in China are required to have a legal representative, though this position often does not exist at companies established in other jurisdictions. In China, the registered legal representative of a company is the main principal of that company and has the authority to represent and bind the company.
[16] See Article 17 of the Measures for the Administration of Data Security.

- Provide the relevant local office of CAC with the data protection plan and incident report in the event a cyber security incident occurs,[17] and
- Accept and process user complaints and reports regarding personal information protection matters.

Each Data Operator will also be required to provide the data protection officer with the necessary resources to carry out all tasks for which such officer is responsible and also ensure that the data protection officer will be allowed fulfill his or her duties independently.[18]

China's draft data protection officer rules resemble some elements of the data protection officer provisions in Section 4 (Data Protection Officer) of the GDPR. China's draft rules, however, do not require Data Operators to register their data protection officers' identity with any supervisory authority. The draft Measures for the Administration of Data Security do indicate that, once those measures are effective, Data Operators will be required to publicly disclose the contact details for their data protection officer.[19]

5. General Requirements of Processing Personal Information

5.1 Explicit User Consent

Prior to any collection, storage, use, transfer, sharing or disclosure of a User's personal information, a Data Operator must obtain explicit, informed consent from the Users for the intended personal information management activities. When requesting consent from Users, a Data Operator should comply with each of the points listed below.

- The Data Operator must ensure that Users have full knowledge of the purpose, method, and scope of the activities regarding the collection and processing of their personal information, which information is generally provided through a publicly available privacy policy;
- User consent must be obtained on a voluntary basis with a specific and clear expression of the User's will;
- Before collecting personal information from a Minor, Data Operators must obtain explicit consent of the Minor's guardian.[20]

[17] For the details of the reporting procedure, please see Section 4.1 of the National Contingency Plan for Cyber Security Incident (国家网络安全事件应急预案), issued by CAC on January 10, 2017.
[18] See Article 18 of the Measures for the Administration of Data Security.
[19] See Article 8 of the Measures for the Administration of Data Security.
[20] See Section 5.4 of the Personal Information Security Specification.

5.2 Principles Relating to Processing of Personal Information

All Data Operator activities involving personal information must comply with the principles of lawfulness, justification and necessity.[21]

- Lawfulness. Only a proper consent can form an effective agreement between the User and the Data Operator.
- Justification. Data Operators must clarify the purpose, means and scope of the agreement between the User and the Data Operator.
- Necessity. Data Operators shall not collect any personal information that is not relevant to the services the Data Operator provides, or collect any personal information in violation of any applicable laws or administrative regulations, or the agreement with Users.[22] The Basic Specification for Collecting Personal Information in Mobile Internet Applications (移动互联网应用程序 (App) 集个人信息基本规范) specifies the categories of necessary information for various kinds of business operations, thereby providing very specific and practical guidance with respect to the necessity principal.[23]

6. Rights of Users

Right to Access, Modify and Delete

Data Operators are also required to ensure Users have the right to access, modify or delete their own personal information held by the Data Operator.[24] Users also have the right to withdraw any consent previously given with respect to their personal information.[25] If a Data Operator violates these User rights, Users could sue the Data Operator, or report the violation to the related administrative authorities. When a Data Operator engages a third party to assist with processing personal information, the third party is required to assist the Data Operator in responding to User requests to exercise these rights.[26]

---

[21] See Article 1035 of the Civil Code, and Article 44 of the Cyber Security Law.
[22] See Article 41 of the Cyber Security Law.
[23] For example, a Data Operator that hosts blogs, forums, and social networking services, would be allowed to collect user account information and some minimal personal information from Users. But if such a Data Operator wants to collect more personal information, like the address, phone number or real-time position of a User, the Data Operator is required to obtain an additional, separate consent from the Users. In other words, collecting this additional information from a User requires a separate consent procedure, rather than just including this consent in the privacy policy that Users clicks through when using an application for the first time. See Basic Specification for Collecting Personal Information in Mobile Internet Applications (移动互联网应用程序(App) 收集个人信息基本规范), issued for public comment by the National Standardization Administration and the State Administration for Market Regulation on October 24, 2019.
[24] See Article 1037 of the Civil Code.
[25] See Article 8 of the Measures for the Administration of Data Security.
[26] See Article 16 of the Minor Protection Rules, and Section 9.1 of the Personal Information Security Specification.

Right to Complain

Users have the right to submit complaints regarding personal information protection matters, and Data Operators are required to establish effective complaint procedures and publicly disclose the contact information of the person or department in charge of addressing these User complaints. Data Operators are required to respond to Users' personal information protection complaints within a specified timeframe, which shall not exceed fifteen (15) business days.[27]

China's rules differ from the GDPR's procedure regarding complaints lodged with a supervisory authority. China requires Data Operators to address User's complaints first. The supervisory authority will only become involved with a User complaint if the Data Operator fails to fulfill its duties.

7. Providing Personal Information to Third Parties

China's personal information protection regime distinguishes among several different ways in which personal information can be shared with third parties, consisting of transferring, sharing or entrusting for processing. When transferring or sharing personal information with a third party, the original Data Operator grants the third party the right to control the User personal information. As a result, the third party becomes a new Data Operator and is required to comply with all relevant rules that apply to Data Operators. The main difference between transferring and sharing is that after transferring only the receiving party will have the right to control the transferred personal information, but after sharing both parties will have independent control over the shared personal information. In contrast, entrusting a third party to process personal information does not involve a change in control rights with respect to the personal information. In all cases, Data Operators are prohibited from providing personal information to third parties in any manner that does not comply with the applicable rules, and those rules differ depending on whether the Data Operator transfers or shares the personal information or whether the Data Operator entrusts a third party to process the personal information.[28]

7.1 Transferring or Sharing Personal Information

[27] See Section 6 of the Methods for Identifying Unlawful Acts of Apps to Collect and Use Personal Information (App 违法违规收集使用个人信息行为认定方法), jointly issued by CAC, MIIT (工信部), Ministry of Public Security (公安部), and State Administration for Market Regulation (国家市场监督管理总局) on November 28, 2019.

[28] See Article 1038 of the Civil Code.

Prior to transferring or sharing personal information, a Data Operator must disclose the details of the proposed transfer or share and obtain User consent. In addition, a Data Operator must conduct a security assessment to ensure that transferring or sharing the personal information will not harm Users' legitimate interests, personal safety or property safety.[29] Although the security assessment criteria is not yet clear, the relevant authorities intend to establish a centralized, unified and efficient data security assessment system.[30] A Data Operator will also be required to enter into a data transfer/share agreement that specifies the responsibilities and liabilities of both parties.[31] The applicable rules do not yet provide detailed requirements for the content of a data transfer/share agreement, but we expect that the requirements will be similar to those for data processing agreement, which we discuss below in the context of entrusting third parties to process personal information.

7.2 Entrusting Third Parties to Process Personal Information

Unlike transferring or sharing personal information, entrusting a third party to process personal information does not require disclosure or consent, provided that the entrusted processing activity does not exceed the authorized scope of processing activities that the Data Operator could have engage in itself based on prior User consent.[32]

Similar to transferring or sharing personal information, before entrusting a third party to process personal information, a Data Operator must complete a security assessment. In addition, the Data Operator and the receiving party must enter into a data processing agreement, which specifies the responsibilities of each party to ensure that User personal information is properly protected.[33] In particular, the data processing agreement must set forth the following obligations of the receiving party:

- Assisting the Data Operator in responding to User requests;
- Taking measures to ensure personal information security, and reporting any personal information data security incidents to the Data Operator;
- Deleting personal information when the contractual relationship is dissolved;
- Being prohibited from subcontracting; and
- Any other obligations required by law or administrative regulation.[34]

[29] See Article 27 of the Measures for the Administration of Data Security, and Article 17 of the Minor Protection Rules.
[30] See Article 20 of the Data Security Law.
[31] See Section 9.2 of the Personal Information Security Specification.
[32] See Article 16 of the Minor Protection Rules, and Section 6.5 of the Online Personal Information Security Instructions (互联网个人信息安全保护指南), issued by the Ministry of Public Security on April 10, 2019.
[33] See Article 16 of the Minor Protection Rules.
[34] These detailed requirements are set forth in Article 16 of the Minor Protection Rules, which applies when a

8. Cross-Border Transfers of Personal Information[35]

China's personal information protection regime includes proposed rules that would create significant barriers to transferring personal information outside of the country. The draft Measures for the Security Assessment for Cross-Border Transfer of Personal Information (个人信息出境安全评估办法) would require a Data Operator to submit an application, security assessment report ("Security Assessment Report") and cross-border data agreement ("Cross-Border Data Agreement") with the data receiver (the "Recipient") to the local office of the CAC before transferring any personal information outside of China.[36] The draft rules specify the application requirements, assessment measures and follow-up records (the "Transfer Records") that apply to the cross-border transfer of personal information. Although these measures are not yet effective, the draft rules are more detailed and comprehensive than the already-effective rules for personal information transfers within China. Recently, CAC launched a pilot project to promote the implementation of the draft measures.[37]

Security Assessment Report Requirement

Security Assessment Reports will be required to include:

- Details on the background, scale, business, finances, credit and online security capabilities of the Data Operator and the Recipient;
- The personal information transfer plan, including the period of time that the transfer will last, the scope of personal information to be transferred, the volume of personal information to be shared, and whether the Recipient will share any of the personal information with third parties after the personal information has been transferred out of China;
- The risk analysis relating to personal information transfer out of China;

Data Operator entrusts a third party to process personal information of Minors. Additional general requirements for data process agreements are set forth in Section 9.1 of the Personal Information Security Specification. We suspect, however, that in practice the requirements set forth in the Minor Protection Rules will apply to all data processing agreements.

[35] For clarification, the word "transfer" used in cross-border transfer means providing personal information to third parties outside China in any manner, including transferring, sharing or entrusting to process. According to the Measures for the Security Assessment for Cross-Border Transfer of Personal Information, the requirements that apply to transferring or sharing personal information are the same as those that apply to entrusting a third party to process personal information. The rules attempt to regulate the activities of Data Operators outside China through binding data agreements. As a result, the requirements that apply to Data Operators outside of China, through the required binding data agreements, are very similar to the requirements that apply to Data Operators inside China.

[36] See Article 4 of the Measures for the Security Assessment for Cross-Border Transfer of Personal Information.

[37] See Overall Scheme for Comprehensively Deepening Innovative Development of Service Trade (全面深化服务贸易创新发展试点总体方案), issued by the Ministry of Commerce on August 14, 2020.

- The measures to protect the personal information security and legitimate rights of the User.[38]

Cross-Border Data Agreement Requirement

The Cross-Border Data Agreement will be required to:

- Specify the purpose, data type and storage period of the cross-border transfer;
- Specify the rights of the Users, including the right to access, modify and delete personal information, and explain how Users can exercise those rights;
- Specify the User right to claim damages against the Data Operator and/or the Recipient if their legitimate rights and interests are harmed;
- Indicate that if the Recipient cannot comply with the Cross-Border Data Agreement due to a change in the legal environment where the Recipient is located, the Cross-Border Data Agreement will terminate or a new security assessment will need to be conducted;
- Indicate that termination of the Cross-Border Data Agreement will not terminate the Recipient's obligation to protect the User personal information, unless the Recipient destroys or anonymizes the personal information;
- Specify that the Recipient shall not transfer the personal information to any third party unless certain conditions are met;[39]and
- Specify the obligations of the Data Operator and the Recipient[40] with respect to compliance with relevant laws and regulations.[41]

---

[38] See Article 11 of the Measures for the Security Assessment for Cross-Border Transfer of Personal Information.

[39] The conditions that must be satisfied before transferring personal information to a third party are as follows: (i) the Data Operator has notified User of the purpose of sharing the personal information, the identity and location of the third party, the types of personal information to be shared with the third party, and the time period that the third party will store the personal information; (ii) the Recipient promises, upon the request of a User, to terminate transmission of such User's personal information to the third party and require the third party to destroy previously received personal information of such User; (iii) the User's consent has been obtained when Sensitive Personal Information is involved; and (iv) if the transfer of personal information damages the User's interest, Data Operator agrees to compensate the User for such damages.

[40] The obligations of the Data Operator are to: (i) provide a User with a copy of the Cross-Border Data Agreement upon request of the User; (ii) provide notice to the Recipient with respect to any User's compliant if requested; and (iii) assume liability for compensation if the Recipient fails to compensate the User for damages caused to the User.

The obligations of the Recipient are to: (i) provide Users with access to their personal information and the ability to respond, modify or delete their personal information; (ii) ensure that the period of time that personal information is stored outside of China does not exceed the timeframe set forth in the Cross-Border Data Agreement; (iii) ensure that performance of the Cross-Border Data Agreement will not violate the data protection rules where Recipient is located; and (iv) notify the Data Operator promptly when there is any change in the data protection rules where the Recipient is located.

[41] See Article 13-16 of the Measures for the Security Assessment for Cross-Border Transfer of Personal Information.

Assessment Measures of CAC

The following factors will be assessed by the CAC when reviewing the Data Operator's cross-border transfer application:

- Whether the transfer complies with the relevant laws, regulations and policies of the PRC;
- Whether the terms of the Cross-Border Data Agreement can fully guarantee the legitimate rights and interests of Users;
- Whether the Cross-Border Data Agreement can be effectively enforced;
- Whether the Data Operator or the Recipient have previously damaged the legitimate rights and interests of any User or experienced any major network security incident; and
- Whether the Data Operator has obtained personal information in a lawful and proper manner.[42]

Personal Information Transfer Records

The following additional requirements apply to the Transfer Records:

- The Data Operator shall retain the Transfer Records for at least 5 years.
- The Transfer Records shall specify the Recipient of personal information, including the Recipient's name, address, contact information.
- The Transfer Records shall specify the types, quantities, and sensitivity level of personal information transferred out of China.[43]

[42] See Article 17 of the Measures for the Security Assessment for Cross-Border Transfer of Personal Information.
[43] See Article 6 of the Measures for the Security Assessment for Cross-Border Transfer of Personal Information.

Exhibit A
China Personal Information Protection Rules

	Laws and Regulations	**Issue Department**	**Issuance Date (YYYY-MM-DD)**	**Effective Date (YYYY-MM-DD)**	**Level of Authority**
1.	Civil Code (民法典)	National People's Congress (全国人民代表大会)	2020-5-28	2021-1-1	Law
2.	Cyber Security Law (网络安全法)	Standing Committee of the National People's Congress (全国人大常务委员会)	2016-11-7	2017-6-1	Law
3.	Data Security Law (数据安全法)	Standing Committee of the National People's Congress (全国人大常务委员会)	2020-7-3	Draft	Law
4.	Personal Information Protection Law (个人信息保护法)	Standing Committee of the National People's Congress (全国人大常务委员会)	2019-10	Draft	Law
5.	Provisions on the Online Protection of Children's Personal Information (儿童个人信息网络保护规定)	CAC (网信办)	2019-8-22	2019-10-1	Department Regulations[44]
6.	Measures for the Administration of Data Security (数据安全管理办法)	CAC (网信办)	2019-6-28	Draft	Department Regulations
7.	Measures for the Security Assessment for	CAC (网信办)	2019-6-13	Draft	Department

[44] Department regulations (部门规章) are rules issued by national level government departments. Department regulations are binding, but with a lower legal effect than laws.

	Cross-Border Transfer of Personal Information (个人信息出境安全评估办法)				Regulations
8.	Methods for Identifying Unlawful Acts of Apps to Collect and Use Personal Information (App 违法违规收集使用个人信息行为认定方法)	CAC (网信办), MIIT (工信部), Ministry of Public Security (公安部), State Administration for Market Regulation (国家市场监督管理总局)	2019-11-28	2019-11-28	Normative Document[45]
9.	Online Personal Information Security Instructions (互联网个人信息安全保护指南)	Ministry of Public Security (公安部)	2019-4-10	2019-4-10	Normative Document
10.	Information Security Technology – Personal Information Security Specification (信息安全技术- 个人信息安全规范)	National Standardization Administration (国家标准化管理委员会), State Administration for Market Regulation (国家市场监督管理总局)	2020-3-6	2020-10-1	National Standard[46]
11.	Information Security Technology – Basic Specification for Collecting Personal Information in Mobile Internet Applications (信息安全技术 - 移动互联网应用程序 (App) 收集个人信息基本规范)	National Standardization Administration (国家标准化管理委员会), State Administration for Market Regulation (国家市场监督管理总局)	2019-10-24	Draft	National Standard
12.	Information Security Technology – Self Assessment Instruction for Personal Information Collection and Use of Mobile Internet Application (信息安全技术-移动互联网应用程序收集使用个人信息自评估指南)	National Information Security Standardization Technical Committee (全国信息安全标准化技术委员会)	2020-7	2020-7	National Standard

[45] Normative documents (规范性文件) can be issued by government departments at various levels. These documents are binding, but with lower legal authority than department regulations.
[46] National standards are not binding rules, but they do provide practical instructions.

Exhibit B
Personal Data Protection Rules Comparative Table

	China Rules	CCPA	GDPR
Protects	"**Personal information subjects**" who are natural persons identified or associated with certain personal information. **Personal Information Security Specification** Section 3.3	"**Consumers**" who are California residents that are either: • In California for other than a temporary or transitory purpose; or • Domiciled in California but currently outside the state for a temporary or transitory purpose. "**Households**" who are people that reside at the same California address, share common devices or services provided by a business, and are identified as sharing the same group account or unique identifier. **Cal. Civ. Code** § 1798.140(g) **11 C.C.R.** § 999.301(h)	"**Data subjects**" who are in the European Union that can be identified in particular by reference to an identifier such as a name, an identification number, location data, online identifiers, or to open or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. **GDPR** Article 3
Regulates	"**Data activities**" that make use of any network to operate on personal information within the territory of	"**Businesses**" that: • Have annual gross revenues in excess of US$25,000,000;	"**Controllers**" located both inside and outside of the European Union who are natural or legal people, public authorities,

	China, including collecting, storing, transmitting, processing, using, transferring, sharing and disclosing personal information. **Minor Protection Rules** Article 2	• Annually buy, receive for commercial purposes, sell, or use for commercial purposes the personal information of 50,000 or more consumers; or • Derive 50% or more of annual revenues from selling consumers' personal information. **Cal Civ. Code** § 1798.140(c)	agencies, or bodies which determines the purpose and means of processing of personal data of data subjects. "**Processors**" located both inside and outside of the European Union who are natural or legal people, public authorities, agencies, or bodies which process personal data of data subjects on behalf of a controller. **GDPR** Article 24 **GDPR** Article 28
Types of Data Covered	"**Personal information**" recorded in an electronic or other form, which can be used, independently or in combination with other information, to identify a natural person's personal identity, including: • Basic personal information • Personal ID information • Personal biometric information • Online ID information • Personal health and physiology information	"**Personal information**" that identifies, relates to, describes, or is capable of being linked to or associated with a particular consumer or household. Non-exhaustive examples include: • Identifiers such as name, postal address, online identifier, IP address, email address, social security number, and other similar identifiers • Characteristics of protected classifications under California or federal law	"**Personal data**" that relates to an identified or identifiable data subject. "**Pseudonymized data**" that is processed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information when the business also: • Keeps any additional information separately; and

	• Personal education/human resources information • Personal asset information • Personal communications information • Personal contact information • Personal internet record • Personal device information • Personal location information • Other information **Personal Information Security Specification** Annex A Schedule A.1	• Commercial information • Biometric information • Internet or electronic network activity information • Geolocation data • Audio, electronic, visual, thermal, olfactory, or similar information • Professional or employment-related information • Education information • Inferences drawn from information **Cal. Civ. Code** § 1798.140(o)	• Implements technical and organizational measures to ensure personal data is not attributed to an identified or identifiable data subject. **GDPR** Article 3
User Rights	"**Right to access**" by the User requires the Data Operator to provide a method for the User to inquire about the User's own information. "**Right to modify**" by the User requires the Data Operator to provide a method for the User to modify or supplement the	The right to "**request to know**" what personal information a business has collected about the consumer or household and to whom the personal information has been disclosed. The right to "**request to delete**" personal information about the consumer or	"**Right of access**" by the data subject to obtain from controller confirmation as to whether or not personal data concerning the data subject is being processed, and access to the personal data in a readable format.

	personal information collected whenever there is a mistake or deficiency. "**Right to delete**" by the User requires the Data Operator to delete all the personal information according to the request of the User. "**Right to withdraw consent**" by the User requires the Data Operator to stop processing personal information of the User, however, the withdrawal will not influence the processing activities carried out before. "**Right to complain**" by the User requires the Data Operator to provide reasonable procedures to deal with the User's complaint.	household that the business has collected from the consumer. The right to "**request to opt-out**" of the sale of a consumer's personal information by a business to third parties. The right to "**request to opt-in**" of the sale of a consumer's personal information by a business to third parties, with affirmative authorization. The right to non-discrimination for the exercise of a consumer's privacy rights.	"**Right to rectification**" by the data subject to obtain from the controller the rectification of inaccurate personal data. "**Right of erasure**" by the data subject to obtain from the controller the erasure of personal data concerning him or her without delay, subject to certain conditions. "**Right to restrict processing**" of personal data by the data subject so that the controller can only continue to process the data subject's personal data with the data subject's consent, subject to certain conditions. "**Right to object**" by the data subject to particular types of processing, including: • Processing necessary for performance of tasks carried out in the public interest; • Processing for direct marketing purposes; and • Processing for scientific or historical research purposes.

	Measures for the Administration of Data Security Article 8 **Personal Information Security Specification** Section 8 **Civil Code** Article 1037	**Cal. Civ. Code** §§ 1798.100 – 1798.125	"**Right to data portability**" by the data subject to transmit personal data provided to a controller to another controller without hindrance. "**Right to lodge a complaint with a supervisory authority**" by the data subject. **GDPR** Articles 15 – 18 **GDPR** Articles 20 – 21 **GDPR** Article 77
Required Notices	The Data Operator shall **disclose the rules** for collection and use, explicitly **indicate the purposes, means and scope** of collecting and using information. Such rules may be included in the **privacy policy** of the website, application, or otherwise made available to the Users.	**"Privacy policy"** made available to consumers describing the business' practices regarding the collection, use, disclosure, and sale of personal information, and the rights of consumers regarding their own personal information. **"Notice at collection"** given by a business to a consumer at or before the point at which the business collects personal information. **"Notice of right to opt-out"** given by a	Controllers must **provide information** to the data subject, in situations where personal data is collected from the data subject or a third-party.

	Measures for the Administration of Data Security Article 7 **Cyber Security Law** Article 41	business informing consumers of their right to opt-out of the sale of their personal information, including an interactive form accessible via a clear and conspicuous link titled "Do Not Sell My Personal Information" on the business's website or mobile application. **"Notice of financial incentive"** given by a business explaining each financial incentive or price or service difference related to providing personal information. **11 C.C.R.** §§ 999.305 – 999.308	**GDPR** Articles 13 – 14
Internal Requirements	No specific requirements on maintaining records of processing activities, unless a cross-border transfer is conducted, in which the Data Operator shall retain the records of personal information transfer for at least 5 years. If the Data Operator collects or processes the data of Minors, it must appoint a "**specific person**" in charge of the Minors' personal information protection.	All businesses handling personal information must: • Inform individuals responsible for handling consumer inquiries about the requirements in the CCPA and how to direct consumers to exercise their rights; and • Maintain records of consumer requests made pursuant to the CCPA and how the business responded for at least 24 months.	Controllers must maintain records of processing activities under its responsibility. Processors must maintain a record of all categories of processing activities carried out on behalf of a controller (Art. 30). Controllers and processors must conduct a **"data protection impact assessment"** where a type of processing uses new technologies and is likely to result in a high risk to data subjects. (Art. 35).

	If any Sensitive Personal Information is collected or processed for commercial purpose, the Data Operator will be required to appoint a "**data protection officer**" in charge of Sensitive Personal Information protection. **Minor Protection Rules** Article 8 **Measures for the Administration of Data Security** Article 17	Businesses that reasonably should know that it buys, receives for commercial purposes, sells, or shares for commercial purposes the personal information of 10,000,000 or more consumers in a calendar year must: • Compile metrics for the previous calendar year as listed in (999.317(g)(1)); • Disclose such metrics by July 1 of every calendar year; and • Establish, document, and comply with a training policy to ensure that all individuals responsible for handling consumer requests and compliance with the CCPA. **11 C.C.R.** § 999.317	Controllers and processors must appoint a **"data protection officer"** in cases where: • The processing is carried out by a public authority or body; • The core activities of the controller or processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or • The core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offenses. **GDPR** Article 30 **GDPR** Article 35 **GDPR** Article 37
Security Requirements	Data Operators shall take technical measures and other necessary measures to ensure the security of personal information collected by them, and	No specific security requirements. Businesses must implement and maintain "reasonable" security procedures and practices appropriate to the nature of the information to protect the personal	The controller and processor must implement appropriate technical and organizational measures to ensure a level of security appropriate to risk, including as appropriate:

	prevent information leakage, damage and loss. **Cyber Security Law** Article 42	information. **Cal. Civ. Code** § 1798.150	• Pseudonymization and encryption of personal data; • The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services; • The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical accident; and • A process for regularly testing the effectiveness of technical and organizational measures for ensuring processing security. Controllers and processors may demonstrate compliance with security requirements by adhering to an Article 40 **approved code of conduct** or an Article 42 **approved certification mechanism.** **GDPR** Article 32
Request Verification	No specific request verification procedures.	Businesses must establish, document, and comply with, a reasonable method for	No specific request verification procedures. Controllers should use all

		verifying that the person making a request is the consumer about whom the business has collected information. Generally, businesses should avoid requesting additional information from consumers for verification and cannot charge a fee to verify the consumer. Businesses should also implement reasonable security measures. **11 C.C.R.** §999.323	reasonable measures to verify the identity of a data subject who requests access. **GDPR** Recital 64
Minors	Processing of personal data of **minors below 14 years of age** must be consented to by the minor's parent or guardian. **Minor Protection Rules** Article 2	Businesses with personal information of **minors under 13 years of age** must establish, document, and comply with a reasonable method for determining and receiving affirmative authorization from the minor's parent or guardian to opt-in to the sale of their personal information. Businesses with personal information of **minors at least 13 and less than 16 years of age** shall establish, document, and comply with a reasonable process for allowing such minors to opt-in to the sale of their personal information.	Processing of personal data of **minors below 16 years of age** must be consented to by the minor's parent or guardian.

		11 C.C.R. §§ 999.330 – 999.332	**GDPR** Article 8
Valuing Data	Data Operators are not require to calculate the value of personal information.	Businesses offering financial incentive or price or service difference must use and document a reasonable and good faith method for calculating the value of the consumer's data. **11 C.C.R.** § 999.337	The GDPR does not require controllers or processors to calculate the value of personal data.
Data Breaches	In the event that personal information has been or is likely to be leaked, damaged or lost, the Data Operator shall immediately take remedial measures, and inform the User in a timely manner and report it to the supervisory authorities. **Cyber Security Law** Article 42	No explicit procedural requirements.	Controllers and processors must notify the supervisory authority. When the data breach is likely to result in a high risk to the rights and freedoms of the data subject, the controller must communicate information about the breach to the data subjects. **GDPR** Articles 33 – 34
Providing Personal Information to Third Parties	"**Transferring or sharing**" personal information requires a Data Operator to: • Disclose and obtain User consent before; • Conduct a security assessment; • Enter into a data transfer/share agreement that specifies the responsibilities and liabilities of both parties.	Businesses shall disclose the categories of third parties with whom they share personal information.	Once personal data is "**transferred or shared**", the receiving party will become a data controller, and therefore will be required to comply with all the requirements applicable to a controller under GDPR. "**Engaging a processor to process**" data on behalf of a controller must be governed

	"**Entrusting for processing**" requires a Data Operator to: • Ensure that the processing activity does not exceed the scope of processing activity that the Data Processor was originally authorized to carry out; • Conduct a security assessment; • Enter into a data processing agreement that specifies the obligations of both parties, the subject-matter and duration of the processing, and the nature and purpose of the processing. The obligations of a processor that must be set forth in the data processing agreement: • Assist the Data Operator in responding to User requests; • Take measures to ensure information security, and give feedback to the Data Operator in case of an information leak;	**11 C.C.R.** § 999.308(g)	by a data processing agreement between the controller and the processor, which sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The obligations of a processor that must be set forth in a data processing agreement: • Process the personal data on instructions from the controller; • Ensure that persons authorised to process the personal data are under an appropriate statutory obligation of confidentiality; • Take all measures required for data security; • Assist the controller to respond to requests for exercising the data subject's rights; • Delete or returning all the personal data to the controller after the processing service ends.

	• Delete personal information when the entrustment relationship ends; and • Any other obligations required by law or administrative regulation. **Personal Information Security Specification** Section 9.1 and 9.2 **Minor Protection Rules** Article 16 and 17 **Measures for the Administration of Data Security** Article 27		**GDPR** Articles 28

Exhibit C
Personal Information Examples[47]

Basic Personal Information	Name, birthday, gender, ethnicity, nationality, family relationship, address, personal phone number, email address
Personal Identity Information	Identity card, military card, passport, driver license, work permit, social security card, residence permit
Personal Biometric Information	Gene, fingerprint, voiceprint, palmprint, pinna, iris, face recognition
Online Identity Information	Personal account, internet protocol address, personal digital certificate
Personal Health and Physiology Information	Personal medical treatment information, such as illness, hospitalization records, medical orders, inspection reports, surgery and anesthesia records, nursing records, medication records, drug and food allergy information, fertility information, medical treatment history, diagnosis and treatment, family medical history, current medical history, history of infectious diseases, as well as information related to personal physical health, such as weight, height, vital capacity
Personal Education/Human Resources Information	Personal occupation, position, employer, degree, education experience, work experience, training record, school transcript
Personal Asset Information	Bank account, authentication information, balance information (balance amount, payment transaction records), real estate information, loan records, credit information, transaction and expense records, cash flow records, virtual currency information, virtual transaction, game key code
Personal Communications Information	Communication records, short message, multimedia message, e-mail, and data that reflects personal communications (often referred to as metadata)
Personal Contact Information	Address book, friend list, group list, email address list
Personal Internet Record	The activities stored in the log, including website browsing records, software usage records, click records, favorite lists
Personal Device Information	Hardware serial number, device media access control address, software list, unique device identification code (such as international mobile equipment identity

[47] See Annex A Schedule A.1 of the Personal Information Security Specification.

	/Android identity/ identifier for advertising /open unique device identifier / globally unique identifier / international mobile subscriber identity of subscriber identification module card, etc.)
Personal Location Information	Tracklog, precise geolocation positioning information, accommodation information, latitude and longitude
Other Information	Marriage history, religious beliefs, sexual orientation, undisclosed illegal and criminal records

Exhibit D
Sensitive Personal Information Examples[48]

Personal Asset Information	Bank account, authentication information, balance information (balance amount, payment transaction records), real estate information, loan records, credit information, transaction and expense records, cash flow records, virtual currency information, virtual transaction, game key code
Personal Health and Physiology Information	Personal medical treatment information, such as illness, hospitalization records, medical orders, inspection reports, surgery and anesthesia records, nursing records, medication records, drug and food allergy information, fertility information, medical treatment history, diagnosis and treatment, family medical history, current medical history, history of infectious diseases
Personal Biometric Information	Gene, fingerprint, voiceprint, palmprint, pinna, iris, face recognition
Personal Indentity Information	Identity card, military card, passport, driver license, work permit, social security card, residence permit
Other Information	Sexual orientation, marriage history, religious beliefs, undisclosed illegal and criminal records, communication records address book, friends list, group list, location information, web browsing records, accommodation information, precise positioning information

[48] See Annex B Schedule B.1 of the Personal Information Security Specification.