大成 DENTONS

China Data Legal Regime

What a foreign investor should know

Grow | Protect | Operate | Finance

January 2022

Whether you face it or not, the economic value of "data" has been recognized and deemed as a new production factor[1] and it affects every public sector, industry, entity, and individual. China has developed a new legal regime on data security and privacy protection. This article will address the key issues which have impact on foreign investors under this new regime in China.

1 At the Fourth Plenary Session of the 19th Central Committee of the Communist Party of China held in October 2019, it was proposed at that time that "a sound mechanism for factors of production such as labor, capital, land, knowledge, technology, management, and data to be evaluated by the market, and remuneration determined by contribution" was proposed.

I. What is data and what is regulated?

1. Overview

Data itself is not a new concept. Data literally is information and it includes all types of documents, files, pictures, videos, or any other media containing any information stored in digital forms or physical forms or other forms. Under the *Data Safety Law of P.R.China* (中华人民共和国数据安全法) effective from September 1, 2021 (***Data Safety Law***), data is defined as any information recorded in electronic means or other means. According to the *Personal Information Protection* (**PIP**) Law of P.R.China (中华人民共和国个人信息保护法) (**PIP Law**) effective from November 1, 2021 personal information refers to all kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the information processed anonymously.

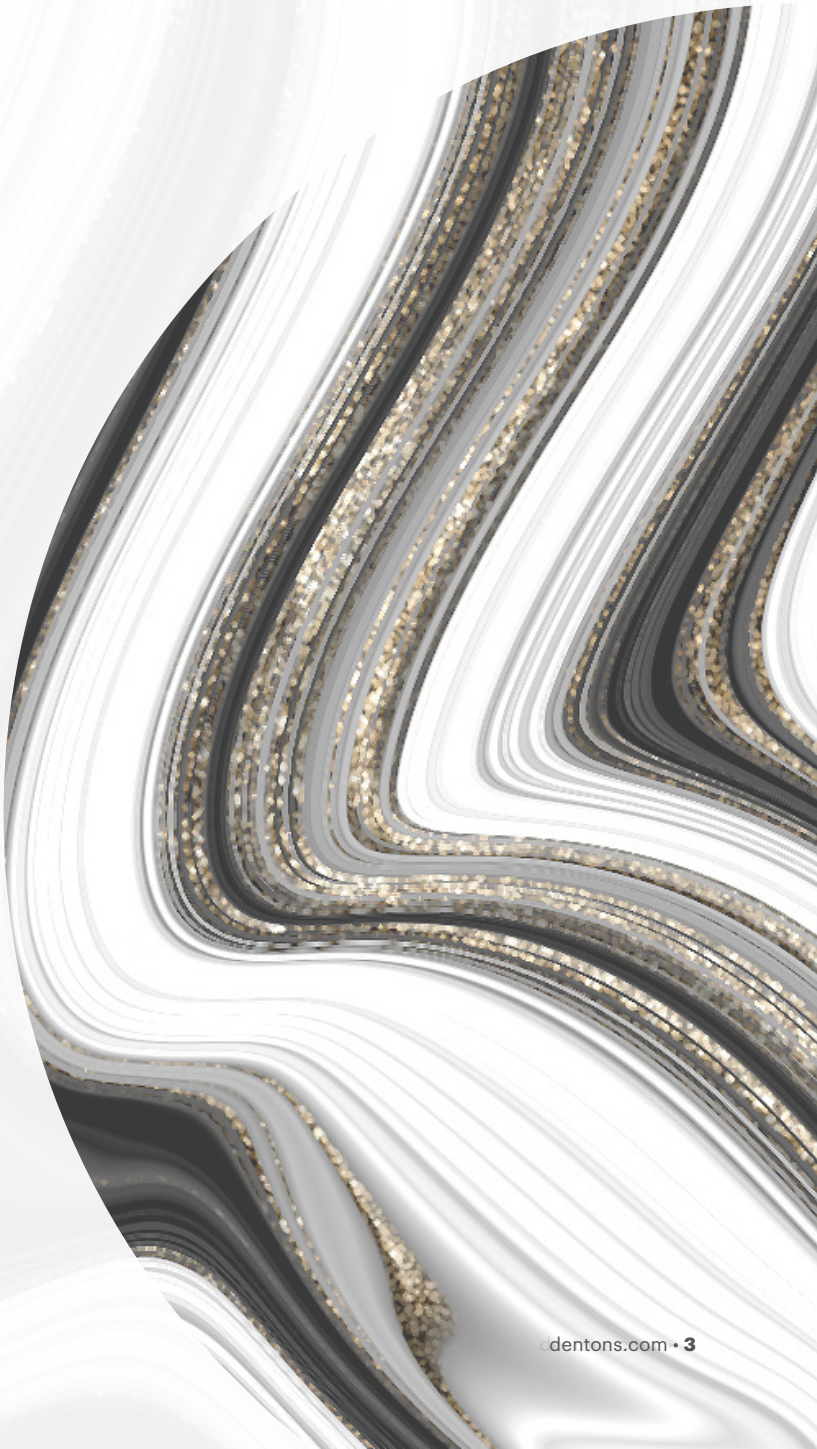
The processing of information or data includes but is not limited to the collection, storage, use, processing, transmission, provision, disclosure and deletion of information.

2. Safety and Privacy are Regulated

It is important to note the main issues to be solved under this legal regime is how to protect the safety of the data and privacy of the individuals, but not restricting the data flow. The fresh new obligations under the laws require a data processor (a new concept as well), to take protection measures for:

i. the national interests, pursuant to the data security laws and rules including
   - *Data Safety Law;*
   - *Network Security Law of P.R.China* (中华人民共和国网络安全法), effective from June 1, 2017 (**Network Security Law**);
   - *Security Protection Regulations for Critical Information Infrastructure* 关键信息基础设施安全保护条例) (**CII Security Rule**), effective from September 1, 2021;
   - *Measures for Cybersecurity Review* (网络安全审查办法) (***CRM Measures***), effective from June 1, 2020, which was superseded by a new amendment issued on December 28, 2021, so called *Measures for Cybersecurity Review* (2021) , to be effective since February 15, 2022;
   - Other relevant rules.

ii. individual privacy, pursuant to the *PRC Civil Code* (中华人民共和国民法典) effective from 2021.01.01, the PIP Law and relevant laws and rules and judicial interpretations on personal information. Note the Data Safety Law is the basic data law that also sets for the principle for PIP protection.



3. Classification of Data Protection and Hierarchical Protection System

Pursuant to the Data Security Law, data are classified as the followings depending on the degree of significance in the economic and social development and seriousness of damage to the national security, public interests or legitimate interests of individuals or organizations if the data is falsified, damaged, disclosed, illegally obtained or illegally used:

i. *Important Data*. According to the Article 21 and 30 of the Data Safety Law, a catalogue of important data is determined and identified by relevant government authorities in each industry and in each region (**Important Data**). An operator of Important Data should do risk assessment periodically on its data processing activities and file such a report to the relevant government authorities for record.

ii. *Core Data*. Under the Article 21 of the Data Safety Law, it refers to the data concerning national security, lifelines of the national economy, people's livelihood, public interests etc. Although the rule is not very clear on the scope of core data, logically it should be interpreted as one type of the Important Data and will require the highest level of security protection.

iii. *A Certain Volume of Personal Data*. According to the Article 21 of the Data Safety Law, important data include personal data. However, personal data will be useful only when it reaches certain volume in terms of big data application. As it has been reflected in the Article 7 of the amended *Cybersecurity Review Measures* (2021), application of overseas listing by a data processor possessing personal information involving over 1 million people will be subject to the Cybersecurity Review led by the Cyberspace Administration of China (**Cybersecurity Review**). In addition, pursuant to a latest draft rule dated November 14, 2021 issued by the Cyberspace Administration of China on *Network Data Safety Administration Regulation (version for public opinion)* (《网络数据安全管理条例(征求意见稿)》), an application of listing in Hong Kong by a data processor involving national security concern will also subject to the Cybersecurity Review.

II. Data Security

1. What is a critical information infrastructure operator (CIIO)?

First of all, data security is relevant to the level of security protection provided for the data generated or collected during the operation of a legal entity. A CIIO is imposed with the highest degree of security protection obligations for this purpose because of its significance meaning to the national economy and security and public interests.

A business operates the following business will be deemed as a CIIO according to the *Security Protection Regulations for Critical Information Infrastructure* （关键信息基础设施安全保护条例）(**CII Security Rule**), effective from September 1, 2021.

> *It operates important network facilities and information systems applied in important industries and fields that may seriously endanger national security, national economy and people's livelihood, and public interests in the event that they are damaged or disabled or their data are leaked. Important industries and sectors, refer to public communication and information services, energy, transportation, water conversancy, finance, public services, e-government, and scientific technology for national defense industry etc.*

A CIIO will be determined and identified by the relevant government authorities in the specific industry, and such a result shall be reported to the authority of public security. Hence, if you have not received such a notification from the relevant government authorities, then you are not a CIIO.

2. National Security Review for Foreign Investment

Obtaining a controlling stake by a foreign investor in critical infrastructure (with no military interests involved) is subject to national security review pursuant to *Measures for the Security Review of Foreign Investments* (Decree No. 37 of the National Development and Reform Commission (**NDRC**) and the Ministry of Commerce (**MOFCOM**), effective as of January 18, 2021 in addition to industrial approvals of relevant government authority.

3. Cross-border Data Transfer

According to the Article 31 of the Data Safety Law, and the Article 37 of the Network Safety Law, the personal information and Important Data generated or collected during the operation of the CIIO shall be stored within the territory of China; and when there is necessity to transfer Important Data out of China, a safety assessment should be conducted in accordance with the rules formulated by the cyberspace administration authority together with relevant departments of the State Council.

4. Data Export

Under the Article 25 of the Data Safety Law, if the data (i) falls under controlled items and (ii) related to the safeguarding of national security interests and the fulfillment of international obligations in accordance with the law, transfer of such information shall also be subject to export control rules.

5. Cybersecurity Review for Critical Information Infrastructure Products or Services Purchased by a CIIO

If a CIIO purchase network products or services that may affect national safety, such purchase will be subject to a Cybersecurity Review to be conducted by a joint working mechanism led by the Cybersecurity Review Office 1 in accordance with the CRM Measures. Note also only 1 months after the CRM Measures take into effective, a new draft of amendment of the measures is circulated for public opinion *Draft Amendment to Measures for Cybersecurity Review* (网络安全审查办法（修订草案征求意见稿）) on July 10, 2021, under the context of Didi's listing in US stock market which stirred the national security concern of cross-border data transfer. And this draft has become the *Measures for Cybersecurity Review* (2021) on December 28, 2021, as mentioned in the section 1.2 above. This amendment is not only applicable to the CIIO, but also a data processor who applies overseas listing and possess personal information involving over 1 million people. Further, according to the latest draft rule on the *Network Data Safety Administration Regulation (version for public opinion)* (《网络数据安全管理条例（征求意见稿）》) *as mentioned in the above section 1.3*, an application of listing in Hong Kong by a data processor involving national security concern is also subject to the Cybersecurity Review. We will closely watch the status and development of these drafts.

6. What Security Obligations A CIIO shall undertake?

Pursuant to the CII Security Rule, a CIIO is required to take security measures ensuring the safety operation of the network facilities and information systems, which basically require the following actions:

i. Creation of a new safety department for data protection ensuring necessary resources of human, financial, and materials in place. A note here is a security background check should be run prior to the appointment of a chief responsible person and the key personnel of this department and necessary support from public security authorities and state security authorities will be provided for such check.

ii. Security measures should be embedded concurrently with design, planning, construction and use of the critical information products, which should cover the life cycle of the products.

iii. Security testing and risk assessment conducted by itself or a cybersecurity service agency at least once a year.

iv. Apply for security review for purchase of network products or services involving national security concern (as set forth in the above paragraph subheading *Cybersecurity Review for Critical Information Infrastructure Products Purchased by a CIIO*)

v. Entering into a safety and confidentiality agreement with a supplier with explicit provisions on technological support, security and confidentiality, and supervising the performance of the supplier.

1 According to Article 4 of Measures for Cybersecurity Review, under the leadership of the Central Cyberspace Affairs Commission, the Cyberspace Administration of China shall establish a national working mechanism for cybersecurity reviews in conjunction with 12 ministries, namely, the National Development and Reform Commission, the Ministry of Industry and Information Technology, the Ministry of Public Security, the Ministry of State Security, the Ministry of Finance, the Ministry of Commerce, the People's Bank of China, the State Administration for Market Regulation, the National Radio and Television Administration, the National Administration of State Secrets Protection and the State Cryptography Administration. In the revised Measures for Cybersecurity Review (2021), China Securities Regulatory Commission, as the 13th ministry is added to the work mechanism. The Office of the Cybersecurity Review is established within the Cyberspace Administration of China, responsible for formulating cybersecurity review systems and standards and organizing cybersecurity reviews.

III. Privacy Protection

1. General

Establishment of a good practice of data protection is necessary as it will help you gain the trust from your employees, your suppliers and your business partners and thus strengthen the ecological development of your organization.

China has modeled the GDPR (General Data Protection Regulation issued by European Union effective as of 25 May 2018) in protection of the privacy interests of individuals with some slight difference summarized below:

- Different from the approach of "adequate" third countries adopted by the EU, China PIP Law requires the transferring party shall enter into a contract with the receiving party ensuring adequate protection measures available under the PIP Law in such a contract for the cross-border data flow;
- The"right to be forgotten" as provided in the GDPR is not the same as the "right to delete"under the PIP Law. Under the PIP law, the right of a data subject asking for deletion is arisen when he/she revokes the consent or when the processing is no longer necessary, or when the information processed is unlawful, but this does not mean a third person can no longer trace the information as that is provided in the GDPR. Furthermore, when an individual revoke its consent, this will not affect the effect of the information processed prior to such a withdrawal.

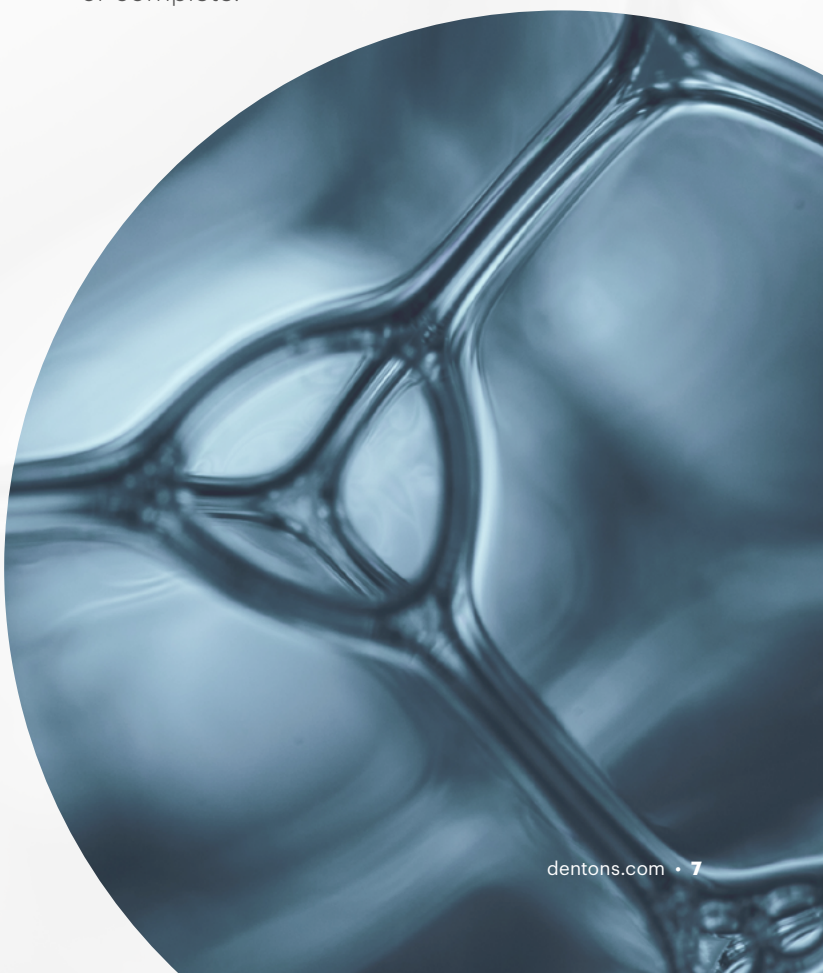
2. Basics about China PIP Law

As such, if your group company have adopted measures consistent with the GDPR, there will not be much difficulty in adjustment to the rules on personal information protection in China. The following statutory requirements under China PIP Law will be a good starting base for you to have a taste of the rules and accommodate your internal corporate rules to the personal data protection under China laws:

i. The purpose of processing personal data is clear and legitimate, and the information processed is minimized for realization of the purpose.

ii. When personal data is collected, more security measures should be taken to protect sensitive information for which the purpose must be specific and the necessity for processing such information should be well grounded. Sensitive information is listed under the PIP Law such as religion, biology identification, disease, financial account, track of whereabouts.

iii. An explicit consent from an individual (i.e., the data subject) is required for first time information collection and subsequent changes of purpose or method of processing when there is an absence of statutory ground for skipping such a consent. Note such a consent can always be revoked. Except for the right to delete as discussed in the second paragraph of section 3.1 above, an individual has also the right to ask for a copy of the information processed, and ask for correction or supplement if the information processed is not accurate or complete.



iv. Under the PIP Law, no consent from an individual is required in the following circumstances:

- where it is necessary for the conclusion or performance of a contract to which the individual concerned is a party, or for the implementation of human resources management in accordance with the labor rules and regulations formulated in accordance with the law and the collective contract concluded in accordance with the law;
- where it is necessary for the performance of statutory duties or statutory obligations;
- where it is necessary for the response to a public health emergency or for the protection of the life, health and property safety of a natural person in an emergency;
- where such acts as news reporting and supervision by public opinions are carried out for the public interest, and the processing of personal information is within a reasonable scope;
- where it is necessary to process the personal information disclosed by the individual concerned or other personal information that has been legally disclosed within a reasonable scope in accordance with the provisions of this Law; and
- other circumstances prescribed by laws and administrative regulations.

v. The length of holding such data should be as short as possible save for otherwise provided under the laws.

vi. The obligations of a data processor will pass to the receiving party due to merger, division, dissolution or declaration of bankruptcy and notifications containing name and contact information of the recipient should be given to the individuals for such changes. The receiving party should bear the same obligations of the data processor as transferred and if the purpose or the method of the information processed is changed, then a new consent from the individual should be obtained.

3. Processing the Information from Employees and Job Candidates by Employers

An employer can certainly process the information required for fulfillment of an employment contract or HR policies of a company in accordance with the laws, however, processing any personal information beyond what is necessarily required for this purpose should always get explicit consent from employees. For sensitive information of employees such as diseases, religion, additional safety measures should be taken to protect such information. For example, when distributing internally employee information containing sensitive information, certain technique measures like generalization of such information should be taken in order not to make the information specific to the individual.

Under the PIP law, the processor can only keep the personal information as short as possible except for where the laws or rules have special provision on such term. Under the PRC Labor Contract Law, an employee contract shall be saved for at least 2 years for record after the termination of the labor contract with this employee. Since the information keeping is a burden for an employer, it is recommended the employer to delete the employee information as soon as possible when it reaches 2 years after the termination.

For job candidates, an employer or interviewer can only collect the information related to the capacity of filling the job duties, and the candidates should be notified how the information should be processed by the employer including the storage, purpose and length of keeping such information. If the purpose or method of processing such information is changed, then explicit consent should be obtained from the candidates. When the time for keeping such information is expired, or the candidates request deletion of their information, such information should be destroyed.

4. Processing the Customers Information

A business entity should update its privacy policy offered to its customers or users from its website, and the product or service agreement entered with consumers or suppliers, following the principles of equality and fairness, good faith, transparency and data minimization, in addition to compliance with the requirement in certain industries such as automobile, and healthcare.

5. Processing Personal Data in Multinational Companies

An international company should be careful to process its China subsidiary's employee information or China individual customers information involving a certain volume of personal data, as this might subject to data safety assessment pursuant to Data Safety Law. Although the exact volume has not been provided in the current effective laws and rules, according to the Article 4 of the draft regulation circulated for public opinion *Drafted Measures for the Security Assessment of Outbound Data* (数据出境安全评估办法（征求意见稿）) on October 29, 2021, prior to provision of such information by China subsidiaries, the following provisions can be taken for reference, although the draft rules yet become effective:

- If the China subsidiary is an operator possessing personal data involving over 1 million people, then any cross-border transfer of data originated or collected in China should be subject to the data security assessment prior to the transfer.
- Transfer of persona data involving over 100,000 people in aggregate, or sensitive information involving over 10,000 people, will also be subject to the cross-border data security assessment.

For the abovementioned cross-border transfer of personal data, unless otherwise statutorily exempted (i) a consent of individual should be obtained, and (ii) a contract should also be placed between the China subsidiary and the parent or its group members ensuring the foreign receiver will provide adequate protection to the data transferred.

YOUR KEY CONTACT PARTNER

Susan(Xiaona) Wang
Partner
Beijing Dacheng Law Offices, LLP.
D +86 189 1057 3469
xiaona.wang@dentons.cn

ABOUT DENTONS

Dentons is the world's largest law firm, connecting top-tier talent to the world's challenges and opportunities with 20,000 professionals including 12,000 lawyers, in more than 200 locations, in more than 80 countries. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and award-winning client service challenge the status quo to advance client interests.

dentons.com

CSBrand-78213-China Data Legal Regime — 12/01/2022