大成 DENTONS

Data Protection Alert

New Developments of China's Restrictions on Cross-Border Transfer of Personal Information Under the PIPL

SEPTEMBER 2021

This document is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. For any specific questions, please contact the partners below.

Co-Chairs

Jet Deng
Partner
Beijing Office
Tel: 010 - 5813 7038
zhisong.deng@dentons.cn

Ken Dai
Partner
Shanghai Office
Tel: 021 - 5878 1965
jianmin.dai@dentons.cn

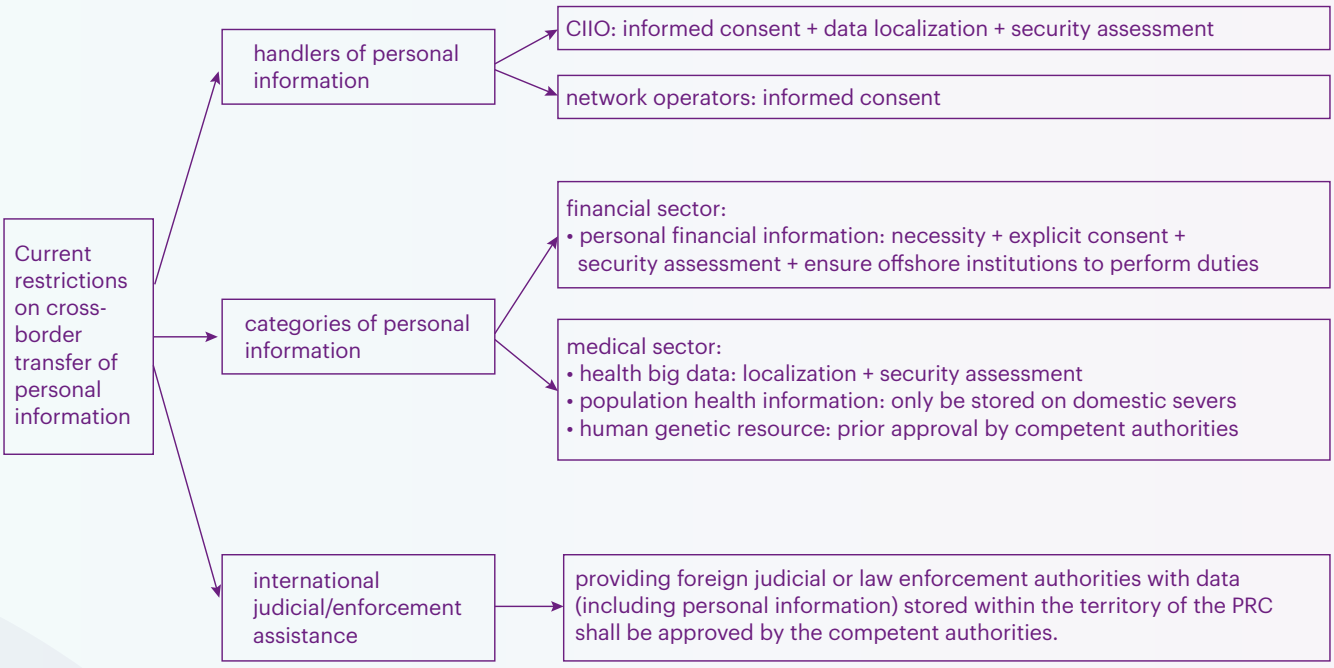
On July 2, 2021, China's top ride-hailing platform Didi Chuxing was announced to be probed for cybersecurity review two days after its IPO in the US, closely followed by two similar probes against other Internet companies that were also US-listed very recently. Several speculations spread on why these companies are subject to cybersecurity reviews, and one of them is related to cross-border data transfer during the overseas listing process. This speculation was further reinforced when the *Cybersecurity Review Measures (Revised Draft for Comment)* (《网络安全审查办法（征求意见稿）》) was released by the Cyberspace Administration of China ("**CAC**") on July 10, 2021, which introduces a mandatory cybersecurity review requirement for any business with personal information of more than one million users that seeks to list its securities abroad.

A month later, on August 20, 2021, the Personal Information Protection Law ("**PIPL**"), the first comprehensive and fundamental law for personal information protection in China, was approved by China's top legislative – Standing Committee of the National People's Congress of China and will take effect from November 1, 2021. Compared with the currently effective laws, the PIPL provides stricter rules in terms of cross-border transfer of personal information

In view of this, this alert intends to sort out restrictions on cross-border transfer of personal information under currently effective laws and the upcoming PIPL. Given that the identification rules of important data are still in the pipeline, relevant restrictions on important data are not involved.

Current Restrictions on Cross-border Transfer of Personal Information

Under the currently effective laws of the People's Republic of China ("**PRC**"), the cross-border transfer of personal information is restricted from three dimensions, including: (1) handlers of personal information; (2) categories of personal information; and (3) international judicial/ enforcement assistance, as shown in the chart below.



A. Cybersecurity Law: Restriction on Handlers of Personal Information

Before November 1, 2021 when the PIPL comes into effect, the Cybersecurity Law （《网络安全法》） ("**CSL**") provides basic rules for personal information handling within the territory of the PRC. Under this law, there are two types of obligors: (i) network operators, essentially anyone who owns or operates a computer network, server or website within the territory of the PRC; and (ii) Critical Information Infrastructure Operators ("**CIIOs**"), a subset of network operators, referring to a more restrictive group of companies in key sectors which are subject to more onerous cybersecurity obligations.

Article 37 of the CSL which provides the basic rules for cross-border data transfer only stipulates relevant obligations of the CIIOs without covering other network operators. Specifically, non-CIIOs only need to fulfill the general requirements for personal information handling - observing the principles of legality, propriety and necessity and obtaining the data subjects' informed consent, while the CIIOs shall undertake two extra obligations, namely (1) storing within the territory of the PRC the personal information and important data collected and generated during its operation within the territory of the PRC ("**data localization**"); (2) conducting security assessment pursuant to the measures formulated by the CAC together with competent departments of the State Council where such information and data have to be provided abroad for business purposes ("**security assessment**"), unless otherwise provided for in laws and administrative regulations.

Since the CIIOs shall bear much heavier obligations than other network operations, the identification of the CIIOs becomes crucial. As for this issue, Article 31 of the CSL provides the definition of the Critical Information Infrastructure ("**CII**"): the CIIs are those in important industries and sectors such as public communications, information service, energy, transport, water conservancy, finance, public service and e-government, etc., which, once damaged, disabled or data disclosed, may severely threaten the national security, national economy, people's livelihood and public interests. However, with this principal definition, network operators still have difficulty in finding out whether themselves can be identified as the CIIOs.

In view of this, Ministry of Public Security released the *Guiding Opinions on Implementing the Graded Protection System for Cybersecurity and the Security Protection System for Critical Information Infrastructure* （《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》） on September 22, 2020, providing that competent and regulatory authorities in charge of important industries and fields shall develop rules for the identification of the CII, and proactively identify and inform the CIIOs. So far, several regulations and standards at the national level regarding the identification of CII are still in the pipeline, but it has been a normal practice for competent authorities of specific sectors to inform the CIIOs in these sectors of their identification results proactively.

It is worth noticing that following the CSL, efforts have been taken to create general rules for all network operators regarding the cross-border transfer of personal information. Specifically, in 2017 and 2019, the CAC released two relevant exposure drafts namely the *Measures on Security Assessment of the Cross-Border Transfer of Important Data and Personal Information (Exposure Draft)* （《个人信息和重要数据出境安全评估办法（征求意见稿）》） as well as the *Measures on Security Assessment of the Cross-Border Transfer of Personal Information (Exposure Draft)*（《个人信息出境安全评估办法（征求意见稿）》）, which intend to extend the security assessment application from the CIIOs to all network operators. However, these regulations are partly conflict with each other, inconsistent with the PIPL and have not yet been brought into operation. It's likely that they would be subject to further amendments soon to be aligned with the upcoming PIPL.


Adobe St

B. Sectoral Regulations: Restrictions on Cross-Border Transfer of Certain Categories of Personal Information in Financial, Healthcare and Other Sectors

In addition to the CIIOs, network operators in certain sectors, especially finance and healthcare, may need to fulfill other sectoral obligations in addition to informed consent for cross-border transfer of certain categories of personal information.

In the financial sector, the cross-border transfer of personal financial information shall be subject to stricter rules. Under the *Notice of the People's Bank of China for Banking Financial Institutes to Get the Personal Financial Information Protection Work Well Done* (《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》) effective as of May 1, 2011, the personal financial information collected within the territory of the PRC shall be stored, processed and analyzed within the territory of the PRC; The banking financial institute shall not provide any domestic personal financial information to an overseas party unless otherwise prescribed by any law or regulation or the People's Bank of China. Accordingly, the outbound of personal financial information is prohibited in principle and allowed only under exceptional circumstances.

As to the exceptions, the recommended, not compulsory specification named *Personal Financial Information Protection Technical Specification* (《个人金融信息保护技术规范》) effective as of February 13, 2020 released by the People's Bank of China may provide some reference. It provides that a financial industry institute may provide personal financial information for an offshore institute (including its headquarters, parent company or any of its branches, subsidiaries and other affiliates necessary for the completion of such business), provided the following requirements are met:

- due to business needs, it is truly necessary to provide the information for an offshore institute;
- the explicit consent of the personal financial information subject should be obtained;
- a security assessment of the cross-border transfer of personal financial information should be carried out to ensure that the data security protection capability of the offshore institute meets relevant security requirements;
- the financial industry institute should ensure and supervise the offshore institute to effectively perform its duties and obligations such as confidentiality of personal financial information, data deletion, and cooperation with case investigations, by signing of an agreement with the offshore institute and conducting on-site inspections, etc.; and
- the national laws and regulations and relevant rules, measures and standards of industry regulatory authorities should be followed.

Moreover, in the healthcare sector, the cross-border transfer of health big data, population health information, and human genetic resources which may include personal information shall also be subject to stricter rules.

- Health big data is required to be stored on the severs within the territory of the PRC and undergo security assessments before cross-border transfer according to the *Administrative Measures on Standards, Security and Services of National Healthcare Big Data (Trial Implementation)* (《国家健康医疗大数据标准、安全和服务管理办法（试行）》) effective as of July 12, 2018 released by the National Health Commission of China.
- Population health information is not allowed to be stored on the severs overseas under the *Population Health Information Management Measures (Trial Implementation)* (《人口健康信息管理办法（试行）》) effective as of May 5, 2014 released by the National Health and Family Planning Commission.
- Human genetic resource is allowed to transfer abroad only under certain circumstances with the prior approval by the competent authority under the *Regulations on the Management of Human Genetic Resources* (《人类遗传资源管理条例》) effective as of July 1, 2019 released by the State Council.

C. International Criminal Judicial Assistance Law & Data Security Law: Restrictions on International Judicial/Enforcement Assistance

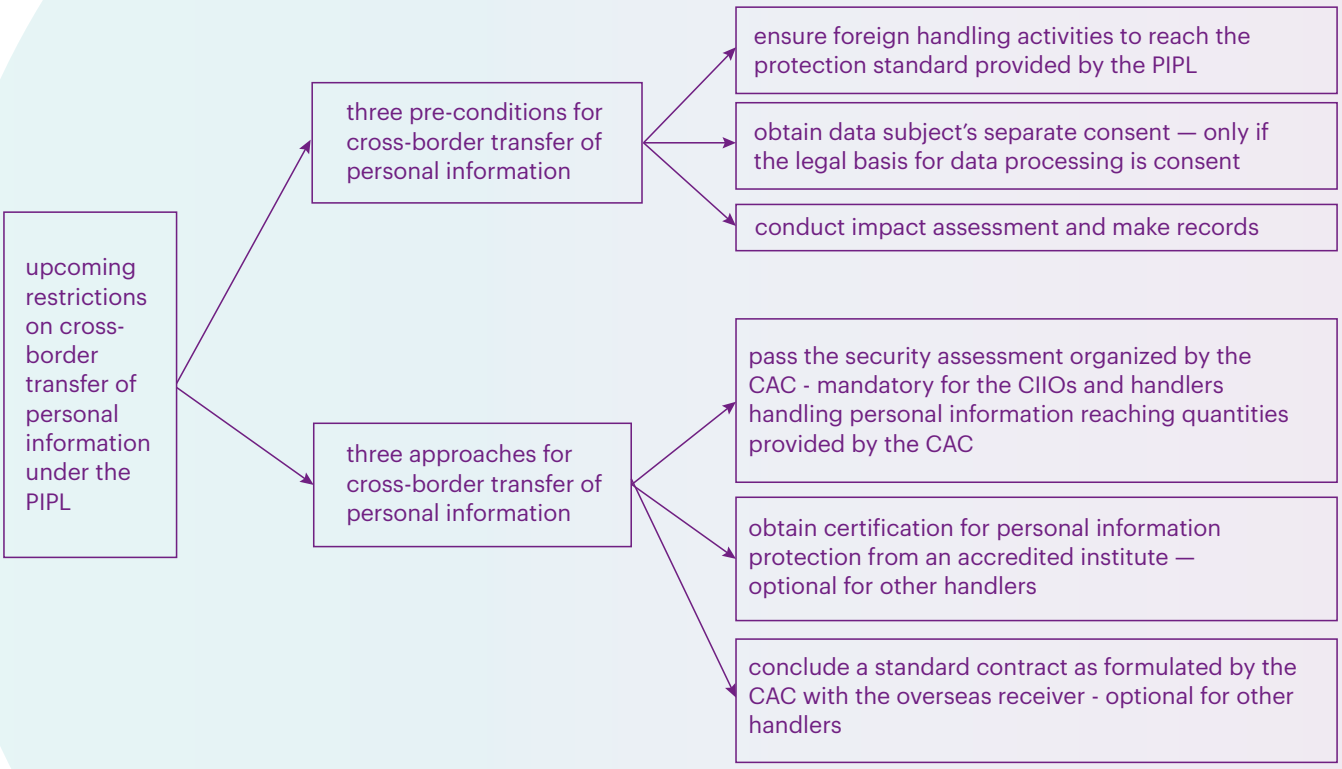
In addition to restrictions from the perspectives of handlers and categories of personal information, the *International Criminal Judicial Assistance Law* (《国际刑事司法协助法》) effective as of October 26, 2018 and the *Data Security Law* (《数据安全法》) effective as of September 1, 2021 provide restrictions from another angle – international judicial/enforcement assistance.

Under the *International Criminal Judicial Assistance Law,* institutes, organization and individuals within the territory of the PRC are prohibited from providing evidentiary materials or assistance in connection with criminal proceedings to foreign countries without approval from the competent authorities. This restriction is regarded as the response to the Clarifying Lawful Overseas Use of Data Act passed by the U.S. Congress in March 2018, which gives U.S. law enforcement authorities the power to request data stored by most major cloud providers, even if it is outside the U.S.

With the Chinese government's intensifying awareness of data sovereignty, the *Data Security Law* that just came into effect introduces consistent but much broader restrictions, extending the restrictive scope from only international criminal judicial assistance to international judicial and enforcement assistance. It provides that no organization or individual within the territory of the PRC may provide foreign judicial or law enforcement authorities with the data stored within the territory of the PRC without the approval of the competent authorities, which undoubtedly include personal information.

Upcoming Restrictions on Cross-border Transfer of Personal Information Under the PIPL

The legal framework for regulating cross-border transfer of personal information under the PIPL to be effective from November 1, 2021 is quite different from that under the currently effective laws. In particular, under the upcoming PIPL, the cross-border transfer of personal information shall meet three pre-conditions and be conducted through one of the three approaches as shown in the chart below.



A. PIPL: Three Pre-Conditions for Cross-Border Transfer of Personal Information

According to the PIPL, transferring personal information outside the territory of the PRC shall meet three pre-conditions, namely (1) adopting necessary measures to ensure foreign handling activities to reach the protection standard provided by the PIPL; (2) obtaining the personal information subject's separate informed consent; and (3) conducting personal information protection impact assessment and recording the handling situation.

(I) COMPARABLE PROTECTION STANDARD OF FOREIGN HANDLING ACTIVITIES

Under the PIPL, personal information handlers (the equivalent of data controllers under the GDPR) shall adopt necessary measures to ensure that foreign receiving parties' personal information handling activities reach the standard of personal information protection provided in the PIPL. However, what measures can be regarded as necessary measures remains to be clarified.

(II) SEPARATE CONSENT

The PIPL stipulates that where a personal information handler provides personal information of an individual outside the territory of the PRC, it shall obtain the individual's separate consent, provided that the individual has been notified of such matters as the name of the overseas receiver, contact method, purpose and methods of handling, personal information categories and ways or procedures for individuals to exercise the rights provided in the PIPL with the overseas receiver and other such matters.

It should be noted that, according to Article 13 of the PIPL, obtaining the data subject's consent is not mandatory if the handling falls within the scope of any other legal basis, for example, the handling is necessary to conclude or fulfill a contract in which the individual is an interested party, or necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded contracts, or the handling is necessary to fulfill statutory duties and responsibilities or statutory obligations. Therefore, it can be inferred that, the separate consent is not required for cross-border transfer if the handling of personal information is not based on the data subject's consent.

(III) IMPACT ASSESSMENT AND RECORDS

Under the PIPL, a personal information protection impact assessment beforehand must also be conducted in relation to the cross-border transfer of personal information. The content of the impact assessment shall include (1) the legitimacy, justifiability and necessity of the purpose and method of handling personal information; (2) the influence on individuals' rights and interests, and the security risks; and (3) whether protective measures undertaken are legal, effective, and suitable to the degree of risk. In addition, personal information protection impact assessment reports and handling status records shall be preserved for at least three years.

B. PIPL: Three Approaches for Cross-Border Transfer of Personal Information

Under the PIPL, cross-border transfer of personal information shall be conducted through one of the three approaches after the three pre-conditions have been met, namely (1) passing the security assessment organized by the CAC; (2) obtaining certification for personal information protection from an accredited institute; and (3) concluding a standard contract as formulated by the CAC with the overseas receiver.

(I) SECURITY ASSESSMENT

Under the PIPL, the CIIOs and personal information handlers handling personal information reaching quantities provided by the CAC can only transfer the personal information overseas if a security assessment organized by the CAC is passed, unless otherwise provided for in laws, administrative regulations and CAC provisions.

Compared with the CSL, the PIPL extends the applications scope of the security assessment from only CIIOs to both CIIOs and other personal information handlers handling personal information reaching quantities provided by the CAC. However, several issues remain to be clarified such as the specific quantity criteria provided by the CAC, agencies that conduct the security assessment, considerations and procedures for the security assessment as well as whether handlers are allowed to voluntarily apply for security assessment.

(II) PROTECTION CERTIFICATION

For handlers that do not fall into the application scope of the compulsory security assessment, personal information can be transferred outside of China through two approaches under the PIPL, one of which is undergoing personal information protection certification conducted by an accredited institute according to provisions by the CAC.

Adopting the protection certification approach conducted by third parties which are professional and neutral under the coordination of the CAC can effectively solve the problem of insufficient manpower of the authorities as well as ensure enough protection for outbound personal information. Similarly, several issues need to be specified through supporting rules such as the list of the institutes that are authorized to conduct certification, considerations and procedures for certification and the valid period of certification.

(III) STANDARD CONTRACT

In addition to obtaining protection certification, handlers that do not fall into the application scope of the compulsory security assessment can also transfer personal information outside of the PRC through the approach of concluding a contract with the overseas receiver in accordance with a standard contract formulated by the cyberspace and informatization department, agreeing upon the rights and responsibilities of both sides under the PIPL, which is similar to the standard contract approach provided by the General Data Protection Law ("**GDPR**") in EU.

It should be noted that a handler is allowed to introduce personalized clauses to the contract concluded with the overseas receiver based on his/her own needs in addition to the standard contract clauses, with the premise that these personalized clauses won't conflict with the standard contract clauses or derogate their protection level.

Compared with the other two approaches, the standard contract approach is much more convenient and is thus more likely to be adopted in practice. It is reported that the CAC has begun drafting the standard contract and may refer to the two sets of Standard Contractual Clauses newly adopted by EU in June 2021.

In addition to the above three approaches, according to the PIPL, where other conditions provided in laws or administrative regulations or by the CAC are met, or where treaties or international agreements that China has concluded or acceded to contain provisions such as conditions on providing personal data outside the borders of the PRC, it is permitted to act according to those provisions.

Outlook for the Implementation of the PIPL

The PIPL which introduces comprehensive regulations on cross-border transfer of personal information applicable to all personal information handlers has been approved by China's top legislative on August 20, 2021 and will take effect from November 1, 2021. However, whether and when these restrictions can be practically implemented is clouded with uncertainty as a bunch of details remains to be clarified, especially those related to three approaches.

Specifically, the PIPL provides personal information localization and export security assessment requirements on the CIIOs and handlers who handle personal information at a volume that exceeds the threshold specified by the CAC. However, the specific rules for defining CII are still pending, and the aforementioned threshold remains to be specified by the CAC. Besides, the specific rules on security assessment conducted by CAC are in the pipeline too, and the two relevant draft measures mentioned before need to be further amended to be aligned with the upcoming PIPL.

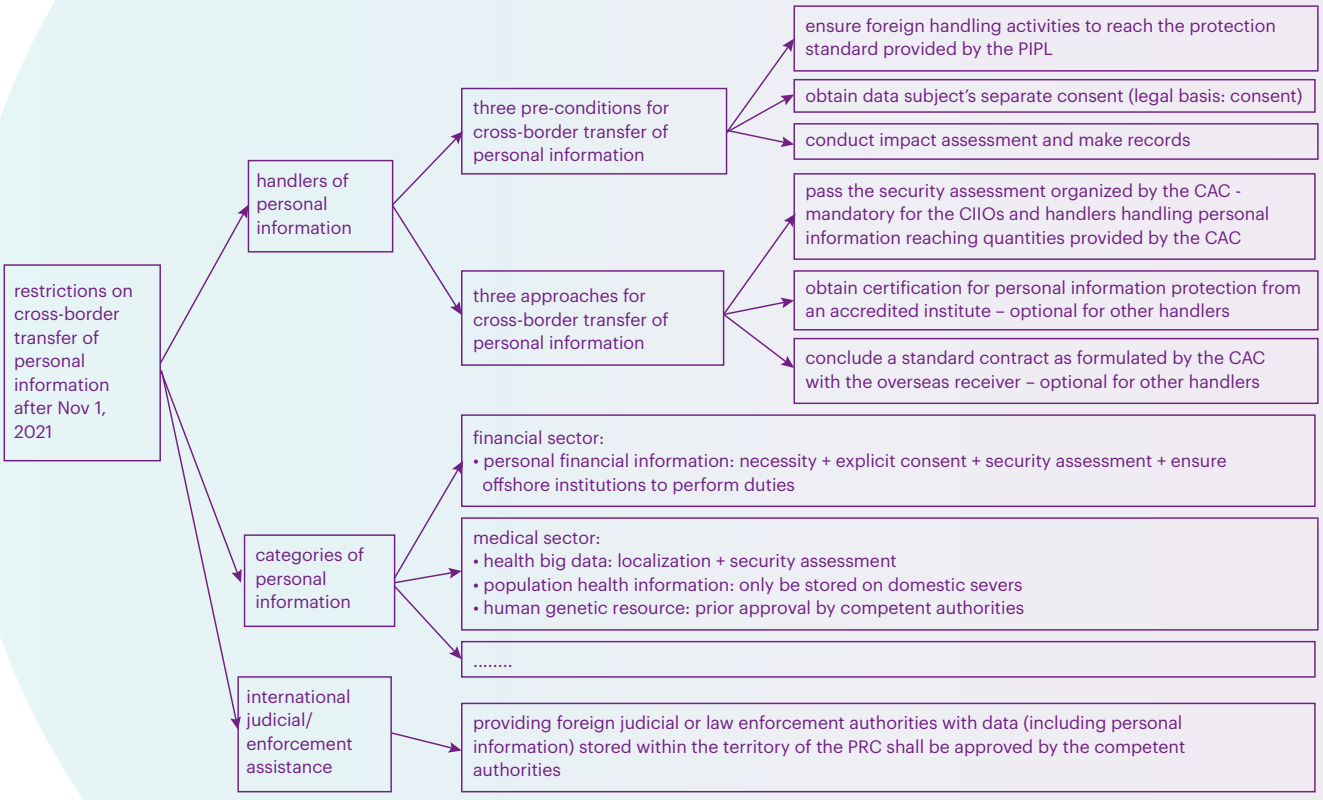
Moreover, according to the PIPL, for the non-CIIOs and handlers who handle personal information at a volume below the threshold specified by the CAC, one of the two approaches – protection certification and standard contract shall be adopted. However, it remains to be seen which accredited institutes are capable of conducting personal information protection certification, how to conduct certification, when will the standard contract be released, etc.

Other issues such as whether the cyberspace administration departments will provide other relevant restrictions on cross-border transfer of personal information through regulations, and what measures can be regarded as necessary measures to ensure foreign handling activities to reach the protection standard provided by the PIPL also need to be clarified.

Conclusion

Since the Didi case, legal standards of cross-border transfer of personal information in China has been getting increasing publicity. Currently, the CSL, sectoral regulations and the *International Criminal Judicial Assistance Law* have provided restrictions from three perspectives, namely (1) handlers of personal information; (2) categories of personal information; (3) international judicial/enforcement assistance. With the enactment of the PIPL to be effective since November 1, 2021, the cross-border transfer of personal information shall satisfy extra requirements, in particular, meeting three pre-conditions and being conducted through one of the three approaches, in the near future, as shown in the chart below.

Though implementation rules remain to be laid down by the follow-up laws and regulations, with the enactment of the PIPL, the framework for regulating cross-border transfer of personal information has been clear. It is recommended for undertakings in China to keep an eye on the legislative progress of specific supporting rules and prepare for the upcoming stricter compliance requirements on cross-border transfer of personal information as soon as possible.




Adobe

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-68188 Data Protection Alert in China — 10/09/2021