DEMYSTIFYING DATA LOCALIZATION IN CHINA: A PRACTICAL GUIDE

Author: Hunter Dorwart
Policy Counsel, Future of Privacy Forum

February 2022

Introduction

With the adoption of the Personal Information Protection Law (PIPL) and the Data Security Law (DSL) in 2021, China has taken important steps to solidify its regulatory framework for cross-border data flows. While this framework is still in flux and incomplete, it contains notable features that help clarify questions around when organizations subject to Chinese data protection laws ("data controllers") must store data locally in China and when they can transfer data abroad.

This report provides an overview of data localization and cross-border transfers under the current Chinese data protection regime. It attempts to give data controllers a better understanding of how the transfers framework operates, the expectations of Chinese regulatory authorities with respect to such transfers, and the specific steps controllers can take for better compliance mapping. It examines provisions of laws formally adopted by the National People's Congress (NPC) and regulatory measures promulgated by ministerial departments.

As this report will show, while the new data protection and data security legal framework solidified and added to pre-existing data localization requirements, it also clarified that data can be transferred or made accessible outside of China if specific conditions are met. Although these localization obligations in China are cumbersome and constitute a barrier to the free flow of data across borders, several pathways remain open for transfers that once understood become easier to implement.

Under Chinese law, data localization is only required in certain circumstances framed around two distinct conceptual pillars: (1) which entity is processing the data; and 2) what type of data is being processed. With respect to the first pillar, **certain special categories of controllers** must store their data in China due to their importance to China's national security and economy, and may only transfer data with the approval of regulatory authorities. For the second, controllers must store **"important data"** in China, and receive approval before transferring such data abroad.

In other circumstances, controllers do not need to store data locally in China but must comply with other transfer requirements. Article 38 of the PIPL sets forth these conditions for lawfully transferring data. Once a controller chooses a transfer mechanism, it must comply with additional transparency obligations. However, it is important to take both the PIPL and DSL requirements into account when deciding whether to localize data or to transfer it.

In order to untangle this complex legal landscape, this Report proposes 10 steps that data controllers can take before deciding to localize or transfer data, with practical advice on how to carry them out:

Step 1 - Determine scope and when data is "transferred" overseas

Step 2 - Evaluate the type of data controller and whether it is a critical information infrastructure operator (CIIO) or a special controller

Step 3 - Determine the type of data to be transferred including whether it is important data

Step 4 - Evaluate whether a security assessment by the CAC is required

Step 5 - Determine whether a cybersecurity review is mandatory

Step 6 - Determine if an exception applies

Step 7 - Choose the transfer mechanism

Step 8 - Check whether an international treaty or agreement is applicable

Step 9 - Obligations for Entrusted Processors (委托处理)

Step 10 (bonus) - Determine whether the transfer is compelled by a foreign judicial or law enforcement body

All these steps are detailed below and accompanied by relevant definitions and explanations. However, it is important to note that this Report does not constitute legal advice. Finally, a flowchart summarizing the proposed steps is annexed to the Report.

Step 1 - Determine scope and whether data is "transferred" overseas

As a preliminary step, data controllers must determine whether Chinese data protection laws apply to them and, if so, whether their processing activities constitute a "transfer" that would trigger further compliance requirements.

Both the PIPL and the DSL apply to "data handling activities" (数据处理活动) within the territory of the PRC, with the former covering "personal information handling" defined as "information that identifies or can identify natural persons" and the latter applying to data handling generally. The definition of "data handling activities" is found in many Chinese legal instruments and mirrors the definition of "processing" under the GDPR. In contrast to the GDPR, these laws apply regardless of whether a data controller has an establishment in China.

Chinese data protection laws also carry an extraterritorial effect, which in practice means data controllers who do not process data in China may nonetheless be subject to Chinese privacy law. Under the DSL, this extraterritorial effect kicks in if data handling activities outside of the territory of the PRC harm the national security or the public interest of China, or the lawful rights and interests of individuals and organizations in China (Art. 2). By contrast, the PIPL will apply to data controllers that process data of individuals within China to:

- Provide products or services to individuals in China
- Analyze and assess the conduct of natural persons in China, or
- In other situations provided by laws or regulations (Art. 3)

Under Article 2 of the draft Online Data Security Management Regulations, data controllers that handle domestic important data will also be subject to Chinese data protection laws. As discussed below, important data generally refers to data that if damaged or leaked could harm China's

national security, public order, or the rights and interests of individuals in China.

Once applicability has been determined, the next question is what constitutes a transfer. Numerous Chinese data laws and regulations refer to "providing information abroad" (向境外提供), but none explicitly specify the activities that are subject to this provision. The 2017 Information Security Technology - Guidelines for Data Cross-Border Transfer Security Assessment (信息安全技术数据出境安全评估指南 (征求意见稿)) defines a transfer in three scenarios:

- When data generated in China is stored outside of China
- When a copy of the data is provided to individuals or organizations that are not under the jurisdiction of or not registered in China, or
- When the data is stored in China but can be accessed and viewed by institutions, organizations, and individuals outside of the country.

While these guidelines remain in draft form, Chinese policymakers may formalize a similar approach in the future through either a technical standard or a regulatory measure. Until this happens, it is currently unclear if data localization in China follows a strict paradigm, as the definition of transfer has not been solidified. Entities that simultaneously store a copy in China and abroad may be considered non-compliant if a data localization rule applies. Additionally, this loose definition carries important implications for data controllers that access data in China through subsidiaries or other affiliated entities. Notably, when third parties outside of China that process data on behalf of data handlers as "entrusted parties" obtain data from a data handler, Chinese regulators will likely deem that a transfer has occurred.

Step 2 - Determine the type of data controller and whether it is a critical information infrastructure operator (CIIO)

Data controllers that fall under the scope of the law and transfer data overseas must then ask whether they are "general" data controllers or whether they fall within a special category of operator, such as, for example, a "critical information infrastructure operator" (CIIO), an "automobile data processor" under the Several Provisions on the Management of Automobile Data Security Regulations[i] (汽车数据安全管理若干规定 (试行)), or a credit reporting service under the Administrative Measures for Credit Investigation Services (征信业务管理办法).

It is important to note that Chinese law does not use the term "general" data controller, but rather establishes a transfer regime that applies in default settings. This report has created the concept of "general" data controller to refer to the baseline option for data transfers under the transfer regime. As discussed below, the architecture of the Chinese data protection framework builds from this baseline and adds stricter requirements depending on the type of controller and the type and level of sensitivity of the data. For a discussion of entrusted parties (i.e., "processors" under the GDPR) obligations) see step nine.

As a default rule, these special data controllers usually must localize data in China, subject to guidance from additional sectoral regulations. This report does not cover every distinct type of controller under Chinese law but rather focuses on one type of important controller - CIIOs. While Chinese regulators will continue to define more narrow categories of data controllers through subsequent regulations and guidelines, recent measures have clarified the compliance path for CIIOs with respect to transfers.

Definition - Under the Critical Information Infrastructure Security Protection Regulations (关键信息基础设施安全保护条例), CIIOs operate "important" network infrastructure and information systems in "important" industries and sectors (Art. 2). Two factors must be considered to determine this:

Whether the data controller processes information in an industry explicitly listed by the Regulation. These include telecommunications, information services, energy, transportation, hydraulic engineering and water utilities, finance, public services, e-government services, national defense science and technology; and

Whether the data controller, once damaged or suffers a data leakage, could severely harm national security, the economy and people's livelihood, or the public interest.

Identification - For business models that do not clearly fall within an enumerated industry, such as cloud providers, ride-hailing services, large internet platforms, or businesses that provide analytic services to critical businesses, determination of CII remains challenging. Currently, the Ministry of Public Security (MPS) oversees the administration of CII, but authorities operating in other sectors will formulate additional rules in other industries. In the likely scenario, such regulations will be issued first as national standards and then incorporated into regulatory measures formulated by key ministries. The test for identifying CIIOs not on the enumerated list has three factors:

- The importance of the business to other critical entities, such as the degree to which the business provides support.
- The extent of the harm to national security, the economy and people's livelihoods, and the public interest if the business is damaged.
- The degree to which the business operates in a field that is essential for the functioning of basic economic and governmental services and the impact of the business on those industries.

Determining the status of a CIIO remains challenging in China and usually involves receiving clarification from regulators. Anecdotal evidence suggests that Chinese authorities have notified individual businesses that they deem them to be CIIOs. Engaging with the appropriate regulator through trusted intermediaries or through social media and other e-government services may be needed and useful.

Transfer Requirements - Under the CSL, CIIOs must store the personal information and other important data they collect or generate in China (Art. 36). If transferring data outside the country is necessary for business purposes, CIIOs must undergo a security assessment in accordance with CAC requirements. Indeed, this is incorporated under Article 36 of the CSL, Article 40 of the PIPL, and Article 4 of the draft Measures for Data Export Security Assessment (Outbound Transfer Guidelines). Note, in theory these provisions only apply to

the processing of personal data and "important" data, and do not cover other generic types of data. However, as discussed below, the current definition of important data is so broad that in practice, all of the data a CIIO generates in China could be deemed "important" simply due to its CIIO status.

Step 3 - Determine the type of data to be transferred including whether it is important data

Data controllers that are not CIIOs or do not fall under sectoral regulations that mandate additional compliance obligations (i.e., "general" data controllers) must then determine the type of data they are transferring. As mentioned above, CIIOs must always store data in China unless they undergo a security assessment with the CAC and receive approval for the transfer. Similarly, under Article 40 of the PIPL and Article 4 of the draft Outbound Transfer Guidelines, controllers that process personal information above a certain threshold or handle important data must also undergo an assessment. Sector-specific regulations may also obligate certain industry participants to receive certification from the CAC before engaging in a transfer.

In each of these scenarios, controllers must store data locally and seek approval prior to sharing data overseas. A transfer also likely includes accessing data that is stored in China from abroad or sharing data with subsidiaries or affiliated offices that operate outside of China. This means that as a default rule, if an entity determines they need to receive a security assessment, they must strictly store data in China.

Personal Information (个人信息)

If the data in question is personal information, the draft Outbound Guidelines provide that controllers who (i) process personal information of at least 1 million individuals or (ii) cumulatively provide personal information of more than 100,000 people or sensitive personal information of more than 10,000 people abroad, must undergo a security assessment by the CAC before sending data abroad. From these draft Guidelines, it is expected that 1 million is also the threshold number under Article 40 of the PIPL.

Important Data (重要数据)

The identification of important data remains unclear. However, a national standard already exists to provide some clarification. The Appendix of the 2017 draft Data Outbound Transfer Security Assessment Guideline lays out 27 categories of important data, largely structured around specific sectoral and industrial uses, but has received much criticism in China as being unwieldy and inefficient. In response, Chinese regulators are currently formulating the Identification Guide of Important Data (信息安全技术 重要数据识别指南), which will help businesses better determine the important data they process.

Definition - Currently, the most comprehensive definition of important data comes from the draft Online Data Security Management Regulations (网络数据安全管理条例 (征求意见稿)). Under Article 73(3)

important data refers to "data that can endanger national security or the public interest once tampered with, destroyed, leaked, or illegally obtained or used." The Regulations provide an illustrative list that includes:

- Government affairs, work secrets, intelligence data and law enforcement.
- Export control data and other data involved in export control items such as core technologies, design schematics, production processes, etc.
- Data stipulated by laws or regulations that needs protection such as national economic operations, important industrial data, and statistical data.
- Data related to the safe production and operation of "important" industries including those listed as being "critical information infrastructure" in addition to customs, taxation, and key systems components and equipment supply chains.
- Basic national data on population, health, national resources, and environment that is required by national departments to meet scale and precision.
- Data relevant to the security of construction and operation of national infrastructure including CII, national defense facilities, military administration areas, and national defense science and technology units.
- Other data that may affect the security of national politics, territory, military, economy, culture, society, science and technology, ecology, resources, nuclear facilities, foreign interests, biology, space, arctic regions, and deep seas.

Identification Process: The definition of important data remains broad and ambiguous, posing challenges for organizations that must determine and classify their own processing activities. The Identification Guide of Important Data clarifies that personal information is not important data for the purposes of classification, but statistical data and derivative data based on massive personal information datasets may qualify. The Identification Guide proposes three steps for identifying important data:

Organizations should first determine when it's necessary to classify important data by examining existing regulations and management policies of the industry. For instance, the Automobile Data Security Regulations proposes its own definition of important data in the context of automobile data.

The next step is to identify and describe the organization's important data. This involves inventorying, determining the purpose of the data and the main security threats they face as well as the risks posed by leakage or harmful use of the data on national security, public order, and/or the rights and interests of individuals in China, and reviewing the process after cataloging.

Finally, organizations must clarify the source and protection measures of the data and any sharing agreements with third-party processors. After completing this process, organizations should share their catalogs with relevant authorities.

Categories of Important Data: The Identification Guidelines divide important data into eight broad categories. These categories do not classify data but rather help firms and

regulators describe the characteristics of important data. Organizations should keep these categories in mind when they identify their important data. These categories include:·

- Economic operation (经济运行)
- Population and health (人口和健康)
- Natural resources and environment (自然资源及环境)
- Science and technology (科学技术)
- Security protection (安全保护)
- Application services (应用服务)
- Government affairs (政务活动)

Step 4 - Evaluate whether a security assessment by the CAC is required

Under Chinese law, certain controllers processing certain data in China must undergo a security assessment by the CAC before transferring data abroad. While provisions in many Chinese data protection measures seem to require data to be stored locally, they usually also contain a mechanism that allows transfer when there is a business need.

In these circumstances, approval from the CAC or other relevant authority will authorize the transfer. For instance, under the People Bank of China's (PBOC) Notice Regarding Effective Protection of Personal Financial Information by Banking Institutions (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 (现行有效)), financial information must be processed in China unless the data controller obtains express consent from the data subject, passes a security assessment by the PBOC, and ensures that the recipient follows the processing agreement.

The draft Outbound Transfer Guidelines provide that the CAC will assess the legality, legitimacy, and necessity of the purpose, scope and method of transfer. This means that the transfer is not explicitly prohibited by laws or regulations and the controller has received consent from the data subject if transferring personal information.

Additionally, the CAC will focus on the security risks involved in the transfer, including possible cyber incidents, the scope of minimization and de-identification, the sufficiency of the transfer mechanism and agreement, the data protection measures taken by the recipient, and the legal environment of the country where the recipient sits. In particular, the CAC will evaluate whether the conditions of the transfer meet the level of data protection standards required in the PRC under Article 38 of the PIPL, which involves considering the power of law enforcement agencies in the recipient country to acquire the data.

Security assessments are valid for two years unless a material change to the (i) purpose, scope, type or duration of transferred data, (ii) the data protection standards of either the sender or recipient of data, or (iii) the legal environment of the recipient countries occurs.

Both the PIPL and the DSL propose the creation of a "whitelist" for data transfers, that would operate as a quasi-adequacy agreement for bilateral transfers in and out of China. The draft Outbound Transfer Guidelines indicate that the CAC security assessment procedure will primarily operationalize this process, especially for transactions involving well-known recipients or destinations such as Hong Kong.

After determining applicability, the type of controller, and the type of data being processed, it is relatively easy to decide whether a security assessment by the CAC is required.

- CIIOs and other "non-general" data controllers ➔ must obtain an assessment for all their data.
- "General" data controllers processing personal information of over 1 million individuals or that provide personal information of 100,000 individuals or sensitive personal information of 10,000 individuals ➔ must obtain an assessment for their personal information.
- "General" data controllers processing important data ➔ must obtain a security assessment for their important data.
- Entities operating in specific industries with sectoral regulations and administrative measures ➔ must check those regulations for tailored guidance.

Step 5 - Determine whether a cybersecurity review is mandatory

The Cybersecurity Review Measures (CRM) 网络安全审查办法 (修订草案征求意见稿))

impose an additional review for certain entities and may prohibit the transfer of data abroad. Notably, Chinese regulators used this review process on Didi Chuxing in July. For a more detailed overview, see our analysis, "Spotlight on the emerging Chinese Data Protection framework: Lessons learned from the unprecedent investigation of Didi Chunxing".[ii]

Under this review process, regulatory authorities will conduct an audit when the processing activities of the data handler, including cross-border transfers, carry potential harm to national security. Of the type of activities that will always mandate a cybersecurity review, the CRM only specifies that CIIOs and "platform network operators" that process personal information of more than 1 million users and list on a foreign stock exchange must undergo the review.

It is unclear how Chinese regulators will use this mechanism going forward. Unlike the security assessment, which focuses exclusively on the risks of the transfer, the CRM is much broader and potentially encompasses a range of activities. This raises questions as to how authorities in China envision the applicability of the security assessment. It is unclear whether the security assessment will primarily target transfers that affect the rights and interests of individuals in China or whether it will also include a strong national security dimension.

If the former, the CRM may be used more readily, especially in cases that involve state secrets or sensitive information directly tied to national security. If the latter, the CRM may become an exceptional regulatory tool used only in extreme circumstances and will not apply to every data transfer. Regardless, it is unlikely the CRM will be a major concern for foreign data controllers and in most cases a cybersecurity review will likely not be required on top of a security assessment.

Step 6 - Determine if an exception applies

At this point, controllers that pass the inquiries mentioned above do not have to store data locally in China. However, certain transfer restrictions under the PIPL may still apply. For this reason, general controllers should determine whether their processing activities fall within an exception to these restrictions. Article 35 of the draft Online Data Security Management Regulations specifies that data handlers who transfer personal information abroad as required for concluding or fulfilling a contract where the data subject is a concerned party do not need to comply with the transfer requirements of Article 38 of the PIPL. Additionally, Article 35 also stipulates a derogation to the transfer requirements in situations when providing personal information abroad is necessary to protect individuals' lives or health or the security or their property.

Note these derogations only apply to "general" controllers in limited circumstances. CIIOs, special controllers, and general controllers transferring important data or personal information above the specified 1 million threshold must still undergo a security assessment by the CAC. In other words, this derogation does not override the draft Outbound Transfer Guidelines but rather modifies the general transfer requirements stipulated under the PIPL.

Notably, Article 38(4) of the PIPL specifies that other laws or administrative regulations may add further transfer mechanisms. The draft Online Data Security Management Regulations represents one such measure. However, these regulations are currently in draft form and the specifics of these provisions remain unclear. Consequently, policymakers in China may modify this provision in the near future and will likely need to add more clarity around how these exceptions will be implemented.

Step 7 - Choose the transfer mechanism

Data controllers that do not need to undergo a CAC security assessment or a cybersecurity review (i.e., "general" controllers) and do not meet the conditions for a derogation must then choose a relevant transfer mechanism under Chinese law. Article 38 of the PIPL stipulates the following conditions for a transfer pursuant to business needs:

- Undergoing a security assessment conducted by the CAC. The draft Outbound Transfer Guidelines provide the most up to date details on this

process (Art. 38(1)). Indeed, this is the same assessment outlined in Step 4. The primary difference here is that "general" controllers may opt for this pathway but are not required to choose it.

- Obtaining third-party certification through a competent government authority according to guidelines issued by the CAC (Art. 38(2)).
- Adopting a standard contractual clause (SCC) developed by the CAC (Art. 38(3)).

The PIPL imposes two additional obligations regardless of the mechanism chosen.

First, data controllers must take measures to ensure that the overseas recipients of the data transfer meet the protection requirements under Chinese law (Art. 38). Note that this provision does not mention the legal environment in which the data controller sits (although a security assessment by the CAC will take this into account).

Second, controllers must obtain separate consent (单独同意) from each of the data subjects. Under the draft Online Data Security Management Regulations, separate consent requires the data handler to obtain personal consent for each item of personal information when carrying out data handling activities and not bundle such consent for multiple items of personal information and multiple processing activities (Art. 73(8)).

Note that Article 36 of the draft Online Data Security Management Regulations specifies that controllers who obtain individual consent separately for transfers of PI at the time of PI collection do not need to obtain additional separate consent as long as the transfer takes place according to the matters related to the original consent.

For each transfer of personal information, the data handler must notify the data subject of the name and contact method of the foreign recipient, the purpose and method of processing, and methods for the data subject to exercise their personal information rights.

The CAC has yet to formulate SCCs or clarify the certification process, although a standardized security assessment may operate as one basis through which the certification process works. Another certification option could involve export control licensing administered by relevant Chinese authorities as stipulated by the DSL. Both options, however, have yet to be finalized. This means that as of writing, "general" data controllers that do not have to undergo a security assessment by the CAC may nonetheless choose to do so depending on the level of risk and the potential cost of noncompliance.

The draft Online Data Security Management Regulations stipulate that all data controllers providing personal information and important data abroad shall compile an outbound transfer security report annually, to be submitted to a district-level CAC before January 31 of each year. The report must include:

- The complete name and contact method of the data recipient and the categories and quantities of the exported data.
- The storage location and retention period of the transfer.
- Any user complaints involving the transfer and subsequent processing of their data.

- Data security incidents and their response situation.
- Onward transfers after the initial export of data.

Finally, controllers must also comply with additional transparency requirements when transferring data abroad. Under Article 39 of the draft Online Data Security Management Regulations, these requirements involve ensuring that the transfer falls within the purpose, scope, and method of handling identified in key documents along the compliance process, such as those indicated in a DPIA, a security assessment, and/or processing or transfer contracts with recipients. Additionally, data controllers must also provide a means of handling transfer-related user complaints, retain daily records of outbound transfer examinations and approval records for three years, and ensure that the details of the transfer, including contemplated onward transfers, are explicitly provided for in the processing agreement and in the notification to the original data subject.

Step 8 - Check whether an international treaty or agreement is applicable

The PIPL provides that "general" controllers who do not need to undergo a security assessment may also rely on an international treaty or agreement that China has signed as the basis for the data transfer (Art. 38). These treaties will likely take the form of agreements specific to data flows or data security. Currently, China has yet to enter into such an agreement. Nevertheless, Article 12 of the PIPL plus China's application to join notable regional trade agreements like the Comprehensive and Progressive Agreement of Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement (DEPA), suggest that the Chinese government is open to exploring this option. Such a treaty would bypass the foregoing steps.

Note that under Chinese data protection law, the Chinese government may take unilateral action to restrict data transfers to certain recipients. This occurs in two primary circumstances. First, when a data controller infringes upon the data protection rights and interests of individuals in China or threatens China's national security by processing certain data, Chinese authorities may prohibit transfers of information to that entity. Second, if a foreign country discriminates or employs prohibitive measures against China with respect to data, China can take equal measures against that country based on actual conditions.

Step 9 - Obligations for Entrusted Processors (委托处理)

Article 21 of the PIPL stipulates that data handlers can entrust certain processing activities to trusted third parties (this mirrors the controller/processor relationship found in the GDPR). The core document outlining the responsibilities of the data handler and the entrusted party is the processing agreement, which must specify the purpose and methods

of processing, the types of personal information handled, the rights and obligations of both parties, and any subsequent processing agreements between the entrusted party and another entity (Art. 21).

The interaction between entrusted handling and China's regime for cross-border transfers occurs largely through the processing agreement, with key compliance obligations revolving around the terms and scope of that agreement. Note, controllers must conduct a risk-assessment for all cross-border transfers to an entrusted party and will have to submit this information to the CAC if a security assessment is required.

Entrusted Processors Obligations - Generally, the entrusted processor has the duty to strictly follow the terms and conditions of the processing agreement. If the agreement itself violates Chinese data protection law, the data controller, not the processor, bears liability. Additionally, the 2020 PI Security Specification stipulates additional requirements. Under these provisions, entrusted processors must:

- Notify the controller if it fails to comply with the agreement due to a special reason.
- Obtain prior authorization for any sub-processing or onward transfers.
- Assist the controller to respond to data subject requests.
- Notify the controller if it cannot provide adequate security or if a security incident occurs, and,
- Not store personal information beyond the terms indicated in the contract, including upon termination.

Processing Agreement - The data controller carries the responsibility to ensure that the transfer complies with relevant requirements, including data localization obligations and, if necessary, obtaining a security assessment. Such obligations also include supervision and oversight.

The draft Outbound Transfer Guidelines and the draft Online Data Security Management Regulations both require the data controller to conduct an internal risk assessment for entrusted processing to identify the potential risks of processing, including those related to cross-border transfers.

Entrusted processors have the responsibility to follow and carry out the processing agreement according to the terms of that agreement and must not exceed the purpose or methods of processing in the agreement. (PIPL Art. 21). In other words, any condition of onward transfers or sub-processing should be contemplated prior to entering into a processing agreement.

The entrusted processor does not bear liability for violations to cross-border restriction provisions (including those that harm data subjects) unless the data collection exception applies (see below) or the processor violates the terms of the processing agreement. The entrusted processor must obtain prior authorization from the controller before entrusting to sub-processors.

Notification Requirements - Under the draft Online Data Security Management Regulations, data controllers must notify the data subject of the name of the foreign recipient, their contact method, the handling purpose, method, and information categories, as well as means for data subjects to exercise their data subject rights (Art. 36). Note, the 2020 PI Security Specification (信息安全技术

个人信息安全规范), indicates that this does not have to be provided if the personal information is de-identified and the controller ensures that the data recipient cannot re-identify the data (Art. 9.2(b)).

Note the data controller does not have to identify sub-processors but must generally notify the data subject that an onward transfer will take place when obtaining consent.

When transferring sensitive personal information, controllers must inform the data subject of the types of sensitive personal information and obtain explicit consent in advance.

Security Assessments - Data controllers must include relevant terms regarding the purpose, method, and scope of the processing agreement in both their internal risk assessments (usually conducted as part of a DPIA), their annual outbound transfers security report, and in the report sent to the CAC when undergoing a security assessment. This requirement indicates that the data controller bears responsibility to ensure that the transfer is compliant with the law. Necessary terms include:

- A certification that the transfer is lawful, proper, and necessary and the risk to national security and the public interest if the recipient leaks or destroys the data.
- The trustworthiness and legal compliance system of the data recipient including their cooperation with foreign government bodies and whether they can effectively protect the data.
- Whether the terms of the processing agreement can effectively restrain the data recipient to fulfill their security protection duties contemplated under the contract.
- Conditions of re-transfer. Note Chinese law does not indicate whether the identities of sub-processors must be disclosed to the authorities, but the data controller must ensure that data recipients use the data according to the terms of the processing agreement and adopt sufficient data security measures.

Data Collection Exception - As stated above, entrusted processors do not have to initiate a security assessment or ensure that the transfer is compliant with Chinese law. However, Article 9.6(b) of the 2020 PI Security Specification introduces one notable exception - when the entrusted party collects personal information on behalf of the data controller and fails to obtain consent from the data subject. In this circumstance, regulators will treat the entrusted processor as a joint controller and therefore impose upon it the responsibilities of the controller.

Step 10 (bonus) - Determine whether the transfer is compelled by a foreign judicial or law enforcement body

Under the PIPL, data controllers cannot transfer data stored in China in response to a foreign government request of data without approval from competent authorities (Art. 41). Competent authorities refer broadly to Chinese regulatory bodies, including those that carry out public security, law enforcement, or other administrative responsibilities. In these circumstances, data controllers must identify the relevant regulations and administrative measures that specify the appropriate regulatory body that must give approval before the transfer.

Conclusion

While China's transfer regime involves myriad laws and administrative regulations, a general framework for compliance is discernable and benefits from detailed regulatory intervention, albeit currently incomplete. In particular, the Chinese government has yet to clarify two specific transfer mechanisms (the certification process under PIPL Article 38(2) and the SCCs under Article 38(3)) and has currently not entered into a treaty or international agreement relevant for data transfers. The CAC is expected to release SCCs in the near term, although specific dates remain unknown. Experience suggests the regulator may issue something when it finalizes the draft Outbound Guidelines, the most recent administrative measure dealing with cross-border transfers released in late 2021.

This report untangles some of the complexity of the new legal framework by proposing and explaining concrete steps organizations can take to lawfully transfer data from China or to ascertain whether they are subject to localization requirements.

First, controllers must determine whether they fall within the scope of Chinese data protection law and whether a transfer is actually happening. Second, data controllers should identify whether they are a "special controller", such as a CIIO, which would automatically trigger a specific compliance path. The next step is to evaluate the type of data being transferred to determine whether it is important data or a type of data that would trigger a pre-approval process under a sectoral regulation or a security assessment by the CAC.

After figuring this out, controllers can determine whether a security assessment by the CAC is required (step four) by following the threshold questions. Fifth, controllers should also ask whether their processing activities are of the type to trigger a cybersecurity review under the CRM or whether an exception applies. If not, the next process involves choosing a transfer mechanism specified under the PIPL. Two of these transfer mechanisms remain unclarified, but the CAC should issue guidelines on both in the future. Seventh, controllers should also determine whether an applicable treaty or international agreement exists between China and their established jurisdiction, as this may provide another mechanism for transfer in addition to those specified under the PIPL. Eighth, entrusted processors do not have the obligation to initiate a security

assessment for their initial or onward transfers and must primarily follow the terms specified in the transfer agreement. Lastly, compelled transfers of data outside of China by a foreign law enforcement body must receive approval from a competent Chinese authority.

Localization vs. Transfers: Flowchart

Step 1: Applicability and Determining Transfer

Processing within China? ➔ Yes

Processing data of individuals within China outside of China for the purpose of (a) providing services in China, or (b) analyzing behavior? ➔ Yes

Processing important data? ➔ Yes

Transfer occurs when:
(i) When data generated in China is stored outside of China
(ii) when data is provided to organizations not in China
(iii) When the data is stored in China but can be accessed outside of the country.

Step 2: Determine Type of Data Controller

"General" controllers ➔ not CIIOs or "special" controllers.

CIIOs ➔ Enumerated industry, damage to national security or people's livelihoods if business is damaged or malfunctions.

"Special controllers" ➔ defined in sectoral regulations or administrative measures (e.g., automobile data processor)

Step 3: Determine Type of Data

Personal information ➔ **identifies** or can **identify** a natural person.

Important data ➔ damage or leakage risks harm to **national security, the public order, or the rights and interest of individuals in China.**

Other types of data ➔ to be further clarified and defined by subsequent administrative regulations.

Step 4: CAC Security Assessment

CIIOs → **must** undergo security assessment for **all** transfers.

"Special controllers" → may **possibly** need a security assessment pursuant to specific administrative measures.

"General processors" →

- **Personal information** of more than 1 million individuals or a cumulative transfer of personal information of **100,000** individuals or sensitive information of **10,000** individuals → **must** undergo a security assessment for transfers of personal information.
- **Important data** → **must** undergo security assessment for transfers of important data.

Step 5: Cybersecurity Assessment

Unlikely in most cases.

CIIOs → must undergo a review.

Domestic controllers processing personal information of at least 1 million individuals **and** listing on a foreign stock exchange → must undergo a review.

Transfers that harm national security → **possibly** need a review (need more clarification).

Step 6 - Online Data Security Management Regulations Exception

"General" controllers who do not need to undergo a security assessment may rely on the health and contractual necessity exception.

Controllers do not need to choose a transfer mechanism when providing **personal information** abroad is necessary to:

1. Fulfill or conclude a contract where an individual is a concerned party
2. Protect individuals' lives or health, or the security of their property.

Step 7 - Transfer Mechanism

"General" controllers that do not need to undergo a security assessment must choose a transfer mechanism.

PIPL Article 38 -

1. Undergoing a security assessment by the CAC (voluntary)
2. Obtaining certification through a competent government authority (unclear)
3. Adopting SCCs issued by CAC (forthcoming)

Additional requirements -

1. Ensure data recipient takes measures to ensure same level of Chinese data protection standards
2. Obtain separate consent for the transfer. This is not necessary if the controller notifies the data subject of the transfer at the time of original collection.

Step 8 - International Treaties and Agreements

Concluded between China and a foreign jurisdiction.

May offer another mechanism for transfer in addition to those specified in Article 38 PIPL. Does **not** mitigate against a security assessment, if required.

No agreements currently in operation.

Step 9 - Obligations for Entrusted Processors

General rule:

- Entrusted processors must follow the terms and conditions of the processing agreement.
- Entrusted processors **do not have** responsibility to undergo a security assessment.
- Data controllers bear the liability for ensuring compliance for transfers, including onward transfers.

Data Collection Exception:
An entrusted processor collects data on behalf of a controller and **fails to obtain consent** from the data subject.

Step 10 (bonus) - Compelled Transfers

Compelled by a foreign judicial or law enforcement body

- Data controllers cannot transfer without pre-approval from Chinese authorities.
- Which authority depends on circumstances specified in additional administrative regulations.

ENDNOTES

[i] https://fpf.org/blog/update-chinas-car-privacy-and-security-regulation-is-effective-on-october-1-2021/ (last accessed February 18, 2022).
[ii] https://fpf.org/blog/spotlight-on-the-emerging-chinese-data-protection-framework-lessons-learned-from-the-unprecedented-investigation-of-didi-chuxing/ (last accessed February 18, 2022).

Future of Privacy Forum
1350 Eye Street NW
Suite 350
Washington, DC 20005
e-mail: info@fpf.org
www.fpf.org