

## CHINA REVAMPS ITS RULES ON CROSS-BORDER DATA TRANSFER

The Cyberspace Administration of China (CAC) released the *Provisions on Regulating and Promoting Cross-border Data Flows* (the **New Provisions**)<sup>1</sup> on 22 March 2024, together with the second edition of the Guidelines for Security Assessment Filings (the **Security Assessment Guidelines**)<sup>2</sup> and the Guidelines for Filing Personal Information Export Standard Contract (the **SCC Guidelines**)<sup>3</sup>, each with immediate effect. The New Provisions introduce long-awaited changes to the current PRC data export regime established under the [Cybersecurity Law \(CSL\)](#), the [Data Security Law](#), the [Personal Information Protection Law \(PIPL\)](#) and related secondary rules (collectively, the **PRC Data Laws**). Companies will need to reassess their PRC data arrangements against the qualitative and quantitative data transfer exemptions and the broader impact of these new developments.

### Recap on PRC Data Export Regime

Prior to the New Provisions, under the existing PRC Data Laws, any export of "Important data" needs to go through a security assessment, and export of personal information (PI) outside of the PRC needs to be conducted via one of the following three schemes (unless the law otherwise permits or exempts the application of such requirements):

- i. security assessment organised by CAC;
- ii. certification by third-party institutions licensed to grant such certifications; or
- iii. execution of [standard contract](#) as formulated and issued by CAC (the **Standard Contract approach**).

Many companies have found it challenging to comply with such requirements on cross-border data transfers. For example, the scope of important data<sup>4</sup> is not clearly defined and can be subject to interpretation. Also, the Standard Contract

#### Key issues

- Certain data export activities could be conducted without the need to complete a security assessment, execute any standard contracts or obtain any certification
- The triggers for security assessment and standard contracts are relaxed
- A centralised online system is established, via which companies could submit filing materials online
- Definition of "important data" will now be expressly set out by competent regulators, providing more clarity to market participants

<sup>1</sup> Available at (Chinese only): [https://www.cac.gov.cn/2024-03/22/c\\_1712776611775634.htm](https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm)

<sup>2</sup> Available at (Chinese only): [https://www.cac.gov.cn/2024-03/22/c\\_1712783131692707.htm](https://www.cac.gov.cn/2024-03/22/c_1712783131692707.htm)

<sup>3</sup> Available at (Chinese only): [https://www.cac.gov.cn/2024-03/22/c\\_1712783131692707.htm](https://www.cac.gov.cn/2024-03/22/c_1712783131692707.htm)

<sup>4</sup> For a more detailed discussion on important data, see our prior briefing on the [Data Security Law](#).

approach requires detailed documentation work, which can be burdensome for companies with rather limited operations in the PRC<sup>5</sup>. Furthermore, the timeframe for completing a filing with the CAC has become increasingly uncertain due to the surge in the number of applications and filing requests submitted to CAC.

We also observe that the PRC government is increasingly aware of the importance of balancing data sovereignty considerations with attracting foreign investment into China, as evidenced by various policies and statements from both central and local governments. The recent action plan to attract foreign investments announced by the PRC State Council<sup>6</sup> specifically highlights data transfer as a critical issue –promoting and facilitating the secure flow of data by foreign-invested enterprises across the border is one of the top priorities of the PRC government.

Against this background, CAC has now completed its consultation and internal procedures and released the New Provisions, aiming to strike a new balance between (a) the free flow of data and (b) data security and interest and rights of data subjects.

### Full Exemptions

According to the New Provisions, data export activities falling into any of the below categories can be conducted without the need to complete a security assessment, execute any Standard Contract, or obtain any certification:

Scenarios	Conditions
No PI or Important Data (Article 3 of the New Provisions)	Data being exported: <ul style="list-style-type: none"> <li>is collected and generated during activities such as international trade, cross-border transportation, academic cooperation, transnational manufacturing and marketing, etc.; and</li> <li>does not constitute PI or important data.</li> </ul>
Pass-through (Article 4 of the New Provisions)	Data export that: <ul style="list-style-type: none"> <li>concerns PI that is collected and generated outside the PRC, processed within the PRC, and exported after processing; and</li> <li>does not introduce any PI collected within the PRC or important data into the dataset being processed/exported.</li> </ul>
Contractual Demand (Article 5(1) of the New Provisions)	Data export where: <ul style="list-style-type: none"> <li>there is a genuine demand to export PI in order to execute and perform a contract; and</li> <li>does not involve important data.</li> </ul>

<sup>5</sup> For a more detailed discussion, see our prior briefing on the [Standard Contracts](#).

<sup>6</sup> See the action plan to attract foreign investments issued by the State Council on 28 February 2024, available here (in Chinese only): [https://www.gov.cn/zhengce/content/202403/content\\_6940154.htm](https://www.gov.cn/zhengce/content/202403/content_6940154.htm)

Scenarios	Conditions
	Typical scenarios for data export out of contractual demand include, based on the New Provisions, cross-border e-commerce, cross-border delivery, cross-border remittances or payment, cross-border account opening, air tickets or hotel reservations, visa processing and examination services.
HR Demand (Article 5(2) of the New Provisions)	Data export that: <ul style="list-style-type: none"> <li>• concerns employees' PI;</li> <li>• are in response to a genuine demand for cross-border HR management under internal labour policies and collective employment contracts formulated in accordance with law; and</li> <li>• does not involve important data.</li> </ul>
Emergency Demand (Article 5(3) of the New Provisions)	Data export where: <ul style="list-style-type: none"> <li>• there is a genuine demand to export PI in order to protect the life, health and property safety of a natural person under emergency; and</li> <li>• does not involve important data.</li> </ul>
De Minimis (Article 5(3) of the New Provisions)	Data export where: <ul style="list-style-type: none"> <li>• the total amount of PI that is not sensitive PI exported by a PI processor that is not a Critical Information Infrastructure Operator (<b>CIIO</b>) since 1 January of the current year concerns less than 100,000 individuals.</li> </ul>
FTZ Exemption (Article 6 of the New Provisions)	Data export that: <ul style="list-style-type: none"> <li>• is conducted by an entity within a Free Trade Zone of the PRC (<b>FTZ</b>); and</li> <li>• concerns data that is not captured by the negative list, which sets out data that is subject to restrictions, as formulated by such FTZ and approved by CAC/other competent regulators.</li> </ul>

For the exemptions covering contractual/HR/emergency demand above, there is an important change compared with the consultation draft of the New Provisions. Specifically, the threshold is changed from "necessary (必须)" for contract execution/performance/HR management/protection of vital interests" to "genuine demand (确需)" for such matters. This is a welcome shift, as the term "necessary" implies that companies must assess whether it could complete such contractual/HR/emergency demand functions without exporting data, yet "genuine demand" does not imply such a pre-condition. While regulatory practice is being formulated, we take the view that this has reflected the central government's announced policy to support cross border data flows between foreign invested enterprises and their head offices.

The HR exemption and the De Minimis exemption, when used together, could be particularly useful for multinational companies (**MNCs**) that export PI of employees and business contacts. However, please note that for sensitive PI of non-employees (e.g., ID of vendor representatives collected from KYC processes, and health information collected by healthcare industry players), the De Minimis exemption is not available. Companies have to assess if any other exemption can be relied upon.

Another notable development is that the calculation period for determining the applicable regime is shortened to one year – previously any amount should be calculated for a two year period starting from 1 January of the previous year.

### Simplified Standard Routes

Under the New Provisions, a PI processor can export data through the execution and filing of the Standard Contract or completion of certification if:

- the PI processor is not a CIIO; and
- since 1 January of the current year, exports:
  - PI (which do not contain sensitive PI) of more than 100,000 individuals but less than 1,000,000 individuals; or
  - sensitive PI of less than 10,000 individuals.

In making the calculation above, any PI exported under any of the exemptions mentioned above shall be excluded.

The Standard Contract route could be preferred over certification for various reasons and is indeed the common choice for MNCs to the extent available. In this regard, the filing requirements and procedures have been greatly simplified under the SCC Guidelines, which have been updated together with the issuance of the New Provisions. The main updates under the SCC Guidelines relate to the following aspects –

- the submission of materials for purposes of filing of the Standard Contract with CAC can be conducted through a centralised online system established at the national level going forward (though the traditional option of on-site submission is still available for companies that are not able or suitable for online submission); and
- the Report on Personal Information Impact Assessment, which is a self-assessment report that needs to be filed together with the Standard Contract, is simplified by removing the requirements on the applicant to, among others –
  - demonstrate its capability to protect transferred PI;
  - provide evidential proof related to the effectiveness of its PI protection measures; and
  - analyse in detail the overseas recipient's processing activities and its local data protection rules.

Please note that the contents of the Standard Contract and other documents needed for the filing with CAC remain unchanged.

## Security Assessment and Clarity on Important Data

Any export of PI or important data by a CIIO is subject to security assessment – this requirement as established by the CSL remains unchanged in the New Provisions.

Other than CIIOs, data export activities that fall into any of the below categories are subject to security assessment by CAC:

- (i) important data is exported;
- (ii) the export involves non-sensitive PI of more than 1,000,000 individuals since 1 January of the current year; or
- (iii) the export involves sensitive PI of more than 10,000 individuals since 1 January of the current year.

Compared with the *Measures on Security Assessment for Data Export* issued by CAC in July 2022, there are three notable changes –

- the requirement for a security assessment on PI export by processors processing PI of more than 1 million individuals, is removed;
- the calculation period is changed from a two-year period (*i.e.*, from 1 January of the previous year) to a one-year period; and
- the validity period for a security assessment is extended to three years from two years.

In addition to the above, a most welcome development introduced by the New Provisions is in relation to the identification of important data. Under Article 2 of the New Provisions, data processors should identify and file important data based on the relevant rules. Unless competent regulators publicly announce or otherwise give notification that data is regarded as important data, companies do not need to treat such data as important data for security assessment purposes.

As a result, data would only constitute important data if it is (a) identified by a company as such and filed with competent regulators, or (b) clearly specified and announced as important data by competent regulators. How a company should identify important data and make the corresponding filing would be subject to the rules separately formulated by industrial and/or local governments – this is in-line with the methodology proposed in the new national standard, the *Data Security Technology – Rules for Data Classification and Grading*, which was submitted for approval on 21 March 2024.

Procedure-wise, the Security Assessment Guidelines that have been updated together with the issuance of the New Provisions also streamline the filing procedures by introducing an online filing platform (with onsite filing procedures kept as a back-up) and simplify the documentation requirements, in particular by reducing the contents to be included in the Self-Assessment Report on Risks Involved in Data Export.

## Other Developments

### *New Exporting Activity*

An important question for data export is -what constitutes an export activity?

This question has been specifically addressed in the Standard Contract Guidelines and the Security Assessment Guidelines to include –

- (i) transferring data collected within the PRC outside of the PRC; and
- (ii) allowing access to data stored in the PRC from outside the PRC.

A third type of data export activity has now been added pursuant to the Security Assessment Guidelines and the SCC Guidelines in their 2<sup>nd</sup> edition - the processing of PI outside the PRC that satisfies Article 3(2) of the PIPL.

To elaborate, Article 3(2) of the PIPL provides for the extraterritorial effect of the law. It sets out what types of processing activity, while taking place entirely offshore, are still subject to the jurisdiction of the PIPL. In broad terms, these activities concern PI of individuals located within the PRC and are for the purpose of providing products or services to, or to analyse or assess the behaviours of, individuals located within the PRC.

It is unclear under this new type of data export as to who is the data exporter and who is the data recipient. For example, the PIPL provides that a company outside the PRC collects data directly from individuals within the PRC to provide services of such entities is caught under Article 3(2) of the PIPL. If the data it collects concerns payment information (which is classified as sensitive PI), of more than 10,000 individuals, should such company execute a Standard Contract, and if so, with whom? An alternative interpretation may be that data export takes place when such company further transfers PI to another entity located outside the PRC, upon which it becomes subject to the requirement of security assessment or the Standard Contract.

As the extraterritorial effect of the PIPL is not much tested, there is so far little clarity on how to apply the data export scenario in an extraterritorial context.

### ***Security Assessment/Standard Contracts already Completed***

Many companies would find themselves no longer required to sign and file a Standard Contract or complete security assessment for its data export activities. However, many of them may have already completed the necessary procedures and thus are, technically, required to complete the corresponding update procedures upon certain changes to the filed information, as may be required by law.

The New Provisions, nevertheless, do not provide how such existing filings/assessments should be dealt with, despite the natural expectation being that, since these filings/assessment procedures are not required *per se* under the New Provisions, any subsequent update requirement should not be applicable to these companies as well.

## **Our Observations**

The New Provisions and the trends represented by the New Provisions are welcome and positive news for MNCs operating in the PRC.

Companies may in particular wish to re-examine –

- the type of data being exported, in particular between PI and sensitive PI;
- the number of data subjects involved; and
- the identity of the data subjects involved, being employees, contractual counterparties, customers, mass population, etc..

Having examined the existing and potential data export activities, companies should then decide on the applicable approach for data export and reassess their international and global data strategies.

It is important to note that, with the greater flexibility granted by cyberspace regulators, companies should pay particular attention to avoid being viewed as "abusing" these exemptions. A good record and appropriate decision-making procedures are thus needed.

Companies should also note that these New Provisions do not dispense with other requirements under the PIPL concerning data export, including, for example, the requirement on transparency, consent, and reporting of data breach (which are indeed re-iterated in the New Provisions).

## CONTACTS



**Stella Cramer**  
Partner

**T** +65 6410 2208  
**E** stella.cramer  
@cliffordchance.com



**Ling Ho**  
Partner

**T** +852 2826 3479  
**E** ling.ho  
@cliffordchance.com



**Terry Yang**  
Partner

**T** +852 2825 8863  
**E** terry.yang  
@cliffordchance.com



**Brian Harley**  
Counsel

**T** +852 2826 2412  
**E** brian.harley  
@cliffordchance.com



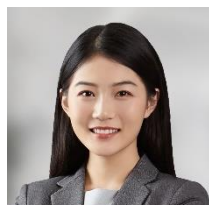
**Clarice Yue**  
Counsel

**T** +852 2825 8956  
**E** clarice.yue  
@cliffordchance.com



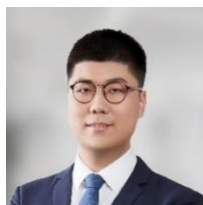
**Jane Chen**  
Senior Associate

**T** +86 10 6535 2216  
**E** jane.chen  
@cliffordchance.com



**Jessy Cheng**  
Associate

**T** + 86 10 6535 4935  
**E** jessy.cheng  
@cliffordchance.com



**Shuai Gao**  
Associate

**T** + 86 10 6535 4915  
**E** shuai.gao  
@cliffordchance.com



**Sharon Zhang**  
Registered Foreign  
Lawyer

**T** +852 2826 3554  
**E** sharon.zhang  
@cliffordchance.com

Any content above relating to the PRC is based on our experience as international counsel representing clients in business activities in the PRC and should not be construed as constituting a legal opinion on the application of PRC law. As is the case for all international law firms with offices in the PRC, whilst we are authorised to provide information concerning the effect of the Chinese legal environment, we are not permitted to engage in Chinese legal affairs. Our employees who have PRC legal professional qualification certificates are currently not PRC practising lawyers. This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

[www.cliffordchance.com](http://www.cliffordchance.com)

Clifford Chance, 33/F, China World Office 1, No. 1 Jianguomenwai Dajie, Chaoyang District, Beijing 100004, People's Republic of China

Clifford Chance, 25/F, HKRI Centre Tower 2, HKRI Taikoo Hui, 288 Shi Men Yi Road, Shanghai 200041, People's Republic of China

© Clifford Chance 2024

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Riyadh • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.