



# China passes provisions to relax the cross-border data transfer regime

April 2024

China has passed provisions which relax the current cross-border data transfer mechanisms. This comes as welcome news to the international business community, especially those with the need to export data from China in the course of their ordinary business activities.

A draft of the New Provisions was initially released in September 2023 for public consultation. The majority of measures introduced by the draft provisions to relax the restrictions on data exports, including the 'blacklist' approach to important data, certain exemptions and *de minimis* thresholds, have been retained in the New Provisions.

On 22 March 2024, the Cybersecurity Administration of China (**CAC**) promulgated the *Provisions on Promoting and Regulating Cross-Border Data Flow* (促进和规范数据跨境流动规定) (**New Provisions**), which take immediate effect. The press conference Q&A by the CAC helpfully clarified the principle that China's restrictions over data export are only meant to apply to personal information and important data and not all types of data that may be transferred across China's borders.

## Position before the New Provisions

In terms of important data, exporting any important data is subject to security assessment. The term "important data" has been defined by various laws, including the *Measures on Security Assessment for Cross-Border Transfer of Data* (数据出境安全评估办法), as data that, once tampered with, destroyed, leaked, illegally obtained or illegally used, may endanger national security, economic operation, social stability, public health and security, etc.. This conceptual definition and the limited guidance otherwise given have exposed many businesses to significant compliance or operational risk.

In terms of personal information, the Personal Information Protection Law (the **PIPL**) requires organisations to rely on one of the following mechanisms (**CBDT Mechanisms**) to transfer any personal information outside of China: (i) security assessment; (ii) protection certification; (iii) China standard contractual clauses (**China SCCs**); or (iv) other mechanism as provided by laws, administrative regulations or the CAC.

Overall, the New Provisions ease the burden on data exporters under certain scenarios by:

1. providing a clear mechanism for the business to identify important data;
2. increasing the quantitative thresholds that would trigger a CBDT Mechanism;
3. setting out scenarios whereby data export is exempted from the CBDT Mechanisms; and
4. stating the period for which security assessments are valid is three years instead of two.

## Key points of note in the New Provisions

### A. Important data

Export of important data will continue to be subject to security assessment under the New Provisions. No exemption or *de minimis* threshold under the New Provisions applies to important data. However, the New Provisions make clear that for data which has not been designated and notified by the relevant departments or regions as important data, or publicly announced as such, data handlers are not required to apply for security assessment for such data before it is exported overseas.

This “blacklist” approach to important data significantly reduces the risks of a company inadvertently exporting important data and should be lauded for its practicality for business operations.

The New Provisions have also increased the validity period of a successful security assessment from two to three years. Within 60 days before the expiration of the validity period, absent circumstances necessitating re-application, the data exporter can apply for an extension of the valid period for another three years.

### B. Exemption scenarios

The New Provisions provide that data exported in the following scenarios is not subject to the CBDT Mechanisms:

- (a) ‘Unregulated’ data – data that is exported as part of international trade, cross-border transport, academic cooperation, and cross-border manufacturing and marketing activities, and does not contain important data or personal information;
- (b) Business necessity – data that is exported in one of the following circumstances:
  - (i) export of personal information that is genuinely needed for the performance of a contract (eg cross-border purchase, cross-border delivery, cross-border payment, flight tickets and hotel reservation, visa application, examination service etc);
  - (ii) export of employee personal information that is genuinely needed for the purpose of human resource management in accordance with legally established employment regulations and collective contracts; or
  - (iii) export of personal information that is genuinely needed to protect the life, health and property safety of a natural person in an emergency.
- (c) FTZ data – data that is outside the negative list in a free trade zone (free trade zones may establish their own ‘negative list’ on data export);
- (d) Non-China originated data – Data that is not collected or generated within China but is provided to China for processing and, during the processing, no domestic personal information or important data is introduced into the set of data.

### **C. *De minimis* threshold**

Unless otherwise exempted under the scenarios described above,

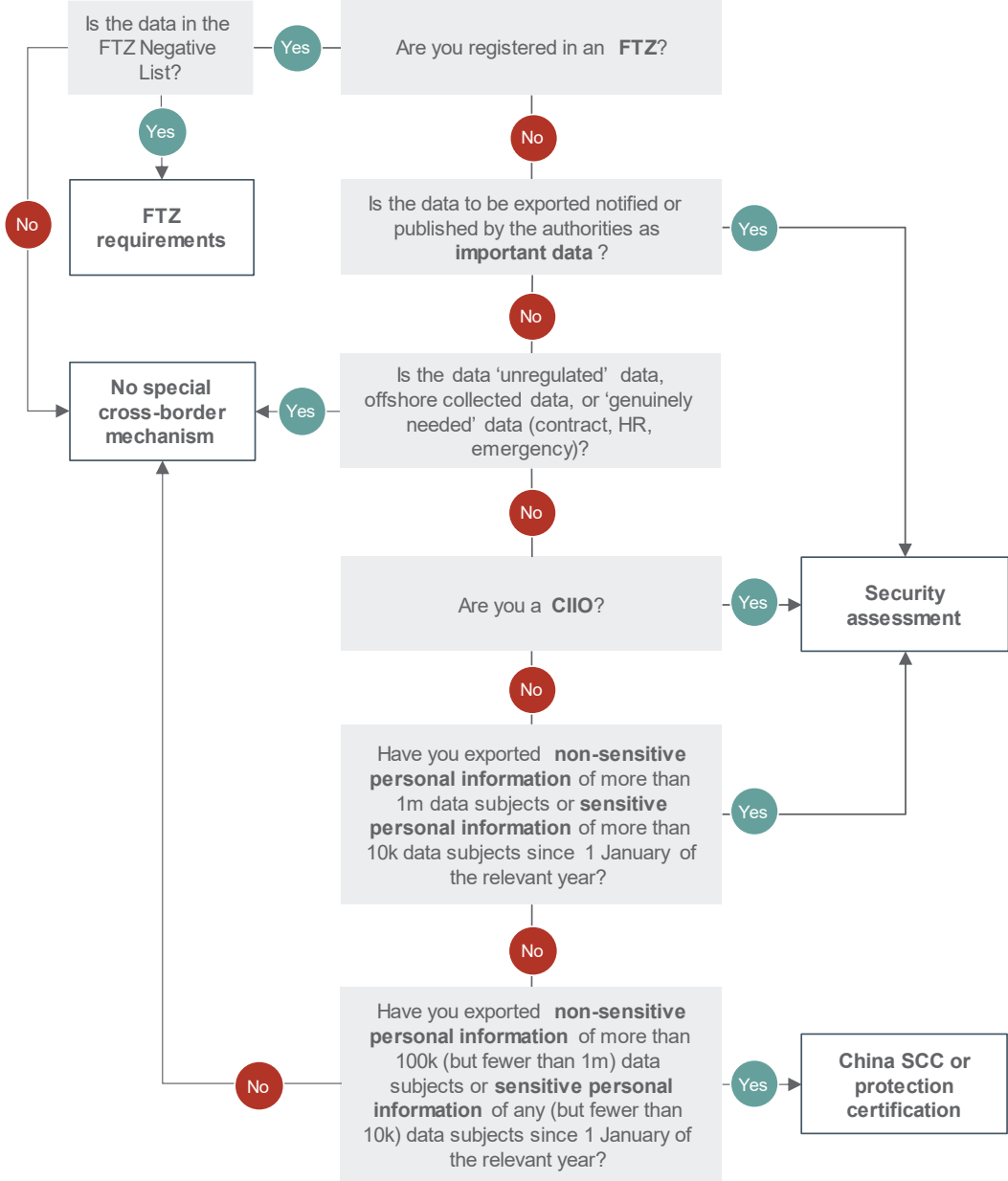
- (a) Organisations are required to complete the security assessment if, since 1 January of the current year, they have:
  - (i) exported sensitive personal information of more than 10,000 individuals; or
  - (ii) exported non-sensitive personal information of more than 1 million individuals.
- (b) Organisations that are not Critical Information Infrastructure Operators (CIIOs) are only required to adopt China SCCs or obtain the security certification if, since 1 January of the current year, they have:
  - (i) exported sensitive personal information of any but fewer than 10,000 individuals; or
  - (ii) exported non-sensitive personal information of more than 100,000 but fewer than 1 million individuals.
- (c) Organisations that are not CIIOs are not subject to any CBDT Mechanism if, since 1 January of the current year, they have not exported non-sensitive personal information of more than 100,000 individuals.

For the avoidance of doubt, the exemptions under Section B above and the *de minimis* thresholds under Section C above do not apply to important data the export of which is always subject to security assessment.

The New Provisions suggest that the CAC is taking a business-friendly approach to data export. They also mean that many organisations may no longer need to complete the security assessment, obtain protection certification or enter into the China SCC and file with the CAC. All organisations should conduct a reassessment of their data export requirements and adjust their compliance framework accordingly. The press conference Q&A also provided useful guidance as to how to transition into the compliance requirements under the New Provisions.

# China Data Update

Provisions on promoting and regulating cross-border data flow



This flowchart is for reference only and does not constitute legal advice.

## Contacts



**Anna Gamvros**  
Partner – A&O – Sydney  
Tel +612 9373 7835  
anna.gamvros@allenoverly.com



**Jane Jiang**  
Partner – A&O – Shanghai  
Tel +86 21 2036 7018  
jane.jiang@allenoverly.com



**Melody Wang**  
Partner – Lang Yue –  
Shanghai/Beijing  
Tel +86 21 2067 6988  
melody.wang@allenoverlyly.com



**Victor Ho**  
Registered Foreign Lawyer,  
Cal – A&O – Hong Kong  
Tel +852 2974 7288  
victor.ho@allenoverly.com



**Susana Ng**  
Of Counsel – A&O –  
Hong Kong  
Tel +852 2974 7015  
susana.ng@allenoverly.com



**Richard K. Wagner**  
Counsel – A&O – Beijing  
Tel +86 10 6535 4309  
richard.wagner@allenoverly.com



**Erin Yang**  
Associate – Lang Yue –  
Shanghai  
Tel +86 21 2067 6905  
erin.yang@allenoverlyly.com



**Zikuan Lu**  
Associate – Lang Yue –  
Shanghai  
Tel +86 21 2067 6850  
zikuan.lu@allenoverlyly.com

Allen & Overy Lang Yue (FTZ) Joint Operation Office

Room 1501-1510, 15F Phase II IFC Shanghai, 8 Century Avenue, Pudong, Shanghai China

Allen & Overy LLP, Shanghai office: Tel: +86 21 2036 7000 FAX: +86 21 2036 7100 www.allenoverly.com

Shanghai Lang Yue Law Firm: Tel: +86 21 2067 6888 FAX: +86 21 2067 6999 www.langyuelaw.com

Allen & Overy Lang Yue (FTZ) Joint Operation Office is a joint operation in the China (Shanghai) Pilot Free Trade Zone between Allen & Overy LLP and Shanghai Lang Yue Law Firm established after approval by the Shanghai Bureau of Justice.

Allen & Overy LLP is a limited liability partnership registered in England and Wales with registered number OC306763. It is authorised and regulated by the Solicitors Regulation Authority of England and Wales.

Allen & Overy LLP is a multi-jurisdictional legal practice with lawyers admitted to practice in a variety of jurisdictions.

The term partner is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings. A list of members' names and of the non-members who are designated as partners is open to inspection at its registered office, One Bishops Square, London E1 6AD, United Kingdom and at the above address. Services in relation to the laws of the People's Republic of China are provided through Allen & Overy LLP's joint operation with Shanghai Lang Yue Law Firm.

Shanghai Lang Yue Law Firm is a general partnership formed under the laws of the People's Republic of China with law firm licence number 23101201410592645 whose registered office is at Room 1514 – 1516, 15F, Phase II, IFC, 8 Century Avenue, Shanghai 200120. It was established after approval by the Shanghai Bureau of Justice. A list of the partners and lawyers of Shanghai Lang Yue Law Firm is open to inspection at its registered office or via the Shanghai Bar Association.

© Allen & Overy LLP 2024. This document is for general information purposes only and is not intended to provide legal or other professional advice. | HKO1: 2006986196.1