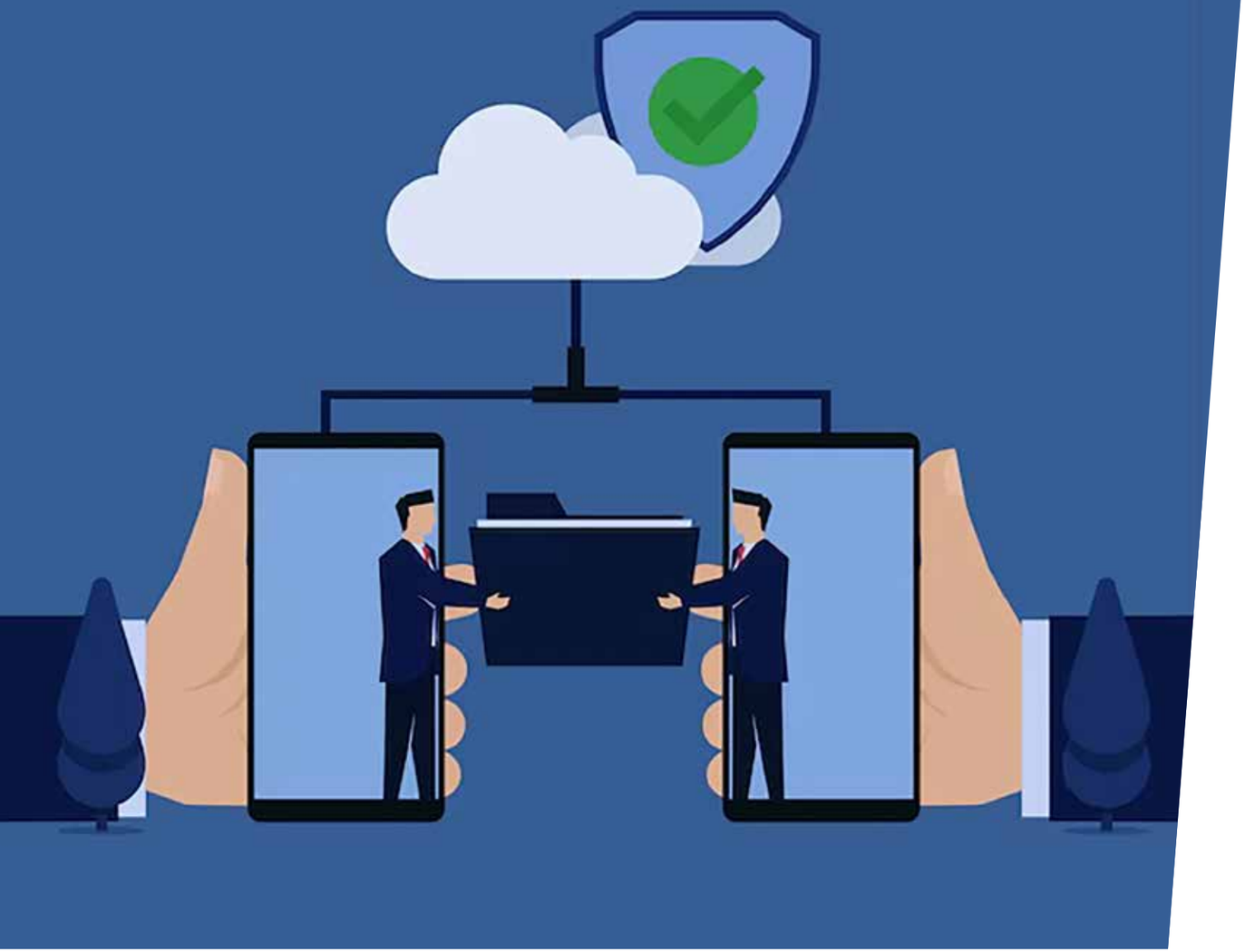
China Releases New Regulation on Cross-Border Data Transfers



> The introduction of the CDF Provisions marks a significant shift by adding a fourth pathway that substantially simplifies the process of exporting data out of China

I. Statutory and Regulatory Background

Six months after the Cyberspace Administration of China (the CAC) the Provisions on Facilitating and Regulating Cross-border Data Flow (CDF Provisions) was officially promulgated on 22 March 2024 with immediate effect.

Prior to the release of the CDF Provisions, multinational corporations (MNCs) with the need to transfer data, especially personal data, out of China, were required to go through one of the three data export mechanisms: (i) the security assessment conducted by the CAC; (ii) the protection certification by a licensed organization; and (iii) the China standard contract (China SCC) for Personal Information Export.

The introduction of the CDF Provisions marks a significant shift by adding a fourth pathway that substantially simplifies the process of exporting data out of China. The Provisions make it clear that in case of any conflicts between the fourth pathway and the existing regulations of the Three Mechanisms that were promulgated before the fourth pathway, the fourth pathway will prevail.

Since its November 1, 2021 effective date, China's Personal Information Protection Law (PIPL) has established the following requirements for transfers of personal information overseas:

- Providing notice to data subjects of the overseas transfer of their personal information;
- Conducting a "transfer impact assessment" (TIA) to assess the risks associated with the data transfer;
- Obtaining the express consent of the data subject to the cross-border data transfer; and
- Executing a standard data contract issued by the CAC.

On February 22, 2023, the CAC published the "Measures for the Standard Contract for the Export of Personal Information" ("Measures"), which, among other things, included the "Personal Information Export Standard Contract" ("Standard Contract") as well as a comprehensive a nd burdensome form for completing the TIA.

On March 15, 2024, the Chinese authorities released the recommended national standard Information Security Technology – Rules for Data Classification and Grading, which will take effect on October 1, 2024.

II. Promoting and regulating, Art. 5 and Art. 6 of the CDF Provisions

For PI, compared to the previously effective regulations and draft solicitations, the new regulations have further relaxed restrictions, and the cross-border PI transfer

DANIEL ALBRECHT
Managing Counsel

> *While maintaining the bottom line of important data and sensitive personal data, the new regulations have greatly relaxed the control over the cross-border transfer of non- sensitive personal data, exempting many common international affairs scenarios from cross-border transfer of PI.*

by a Non-Critical Information Infrastructure Operator of less than 100 thousand per year (excluding *Sensitive Personal Information* (SPI) and *Important Data*) is also exempted (Art. 5), while the quantitative limitation in the draft for soliciting opinions is 10 thousand. This greatly reduces the burden on businesses that do not handle large amounts of PI.

For *important data*, government has officially introduced the "Data Classification and Grading Requirements", the Appendix G of which specifies guidelines for identifying *important data*.

The new regulations officially grant the governments of each free trade zone the right to take the lead by setting up negative lists that can be adjusted and updated in a timely manner, creating a more convenient cross-border data management environment for enterprises in the zone (Art. 6).

1. Important Data and the Security Assessment, Art. 2 of the CDF Provisions

According to the CDF Provisions, unless a data handler has been notified by the CAC that the data it processes constitutes "important data", or the CAC otherwise publicly classifies the data as "important data", the data handler is not required to undergo a security assessment on the basis that it processes "important data" (Art. 2). The recently released "Data Security Technology-Provisions on Data Classification and Grading" provide general rules for data classification and grading, and guidance on identification of important data.

2. Transfers Triggering Application for Security Assessment, Art. 7 of the CDF Provisions

According to the CDF Provisions, if data is transferred outside of China in one of the following scenarios, the data handler is required to apply for security assessment:

- where a *Critical Information Infrastructure Operator* (CIIO) transfers any PI or important data outside of China (Art. 7 I (1)); or
- where a data handler (excluding a CIIO) transfers *important data* or PI of over 1 million individuals (excluding SPI), or SPI of over 10,000 individuals (Art. 7 I (2)).

3. Transfers Triggering Execution of the Standard Contract or Certification of Protection of Personal Information, Art. 8 CDF Provisions

According to the CDF Provisions, where a data handler (excluding a CIIO) transfers PI (excluding SPI) of between 100,000 and 1 million individuals, it should execute the SCC or pass the certification of protection of *personal information*.

4. Exempt Processing Activities Art. 3, Art. 4 and Art. 5 of the Provisions

The Provisions define the following six processing activities as exempt from the application for security assessment, the execution of the SCC, or passing the certification of protection of personal information:

- transfers arising from international trade, cross-border transportation, academic cooperation, transnational manufacturing, marketing, and other activities, that do not involve PI or "*important data*" (Art. 3);
- transit data (i.e., transfers of PI not collected and generated within the territory of China but only processed in China) provided that no PI or *important data* collected in China are added to the transit data during the processing in China (Art. 4);
- transfers necessary for concluding and performing a contract to which the individual is a party, such as cross-border shopping, cross-border shipping, flight and hotel reservations, cross-border remittance and visa processing (Art. 5 I (1));
- transfers of employee *PI necessary* for HR management to comply with employee policies formulated in accordance with the law of China and with the collective contract executed in accordance with the law of China (Art. 5 I (2));
- transfers of *PI necessary* for the protection of a natural person's life, health or property safety in emergency situations (Art. 5 I (3); and
- where a data handler (excluding a CIIO) transfers PI of less than 100,000 individuals (excluding SPI) outside of China during a year (beginning January 1) (Art. 5 I (4)).

III. Continued Rules

The CDF Provisions do not exempt Data Exporters from other compliance requirements for cross-border data transfer under the PIPL. "*important data*" is defined as such data that once tampered with, damaged, leaked or illegally obtained or used may harm the national security, economy, social stability, public health or security. While this obligation remains unchanged, the Provisions clarify that, if the data to be transferred abroad has not been publicly announced by competent regulators, or specifically notified to the *data exporter as important data*, there is no need to undergo the Security Assessment.

Compared with cross-border transfer of *personal information,* Chinese regulators are less likely to relax the restrictions on transferring important data out of China.

IV. Summary

In summary, while maintaining the bottom line of important data and sensitive personal data, the new regulations have greatly relaxed the control over the cross-border transfer of non- sensitive personal data, exempting many common international affairs scenarios from cross-border transfer of PI.

With the Provisions finally settling down, many companies are now facing practical implementation questions. Companies must engage in regular assessments of their catalogues of *core data, important data* and *general data,* ensuring alignment with evolving regulatory benchmarks. It is essential to monitor major changes to business scenarios and plan data processing activities accordingly. Business organizations are strongly advised to closely monitor developments in legislation and enforcement related to data protection and security in China.

ABOUT THE AUTHOR

Author: Daniel Albrecht
Designation: Managing Counsel

Daniel Albrecht is a German attorney at law and Managing Counsel of Starke. He is also member of the board of the German Chamber of Commerce in North China, Supervisory Board member to the European Union Chamber of Commerce in China, external expert for the EU China IPR SME Helpdesk and arbitrator at the Qingdao Arbitration Commission, member of International Trade Committee of the European Communities Trademark Association (ECTA) and also member of the Expert Tank of the Guangdong-Hong Kong- Macao Greater Bay Area International IP Talent Port. He published several articles about Chinese IPR, data protection law and E-Commerce matters. His clients comprise foreign and foreign-invested companies in different areas. His first professional encounter with China was in 2004 as a law clerk.