# Measures on the Security Assessment of Cross-Border Data Transfer

Dan Young Business Consultancy — www.danyoungcpa.com

Unofficial English translation prepared for reference only. The official Chinese text prevails.

## Measures on the Security Assessment of Cross-Border Data Transfer

### Article 1

These Measures are formulated in accordance with the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China, and other applicable laws and administrative regulations, for the purpose of regulating cross-border data transfer activities, protecting personal information rights and interests, safeguarding national security and the public interest, and promoting the lawful, orderly, and free flow of data.

### Article 2

These Measures shall apply to security assessments conducted where a data processor provides data collected and generated during operations within the territory of the People's Republic of China to recipients outside the territory. These Measures shall also apply where data collected and generated within the territory of the People's Republic of China by a data processor, which is stored within the territory, is accessed, queried, downloaded, or exported by an institution, organization, or individual outside the territory.

### Article 3

Data processors shall, when providing data outside the territory, comply with laws and administrative regulations, fulfill data security protection obligations, and ensure the legality, propriety, and necessity of the cross-border data transfer. Data processors shall take technical and other necessary measures to ensure the security of the cross-border data transfer.

### Article 4

Under any of the following circumstances, a data processor shall apply to the national cyberspace administration authority for a security assessment of the cross-border data transfer:

(1) where a data processor provides important data outside the territory;

(2) where a critical information infrastructure operator or a data processor processing personal information of more than one million individuals provides personal information outside the territory;

(3) where a data processor has provided personal information of 100,000 or more individuals or sensitive personal information of 10,000 or more individuals cumulatively outside the territory since January 1 of the previous year; or

(4) other circumstances requiring a security assessment of cross-border data transfer as prescribed by the national cyberspace administration authority.

### Article 5

Before applying for a security assessment of cross-border data transfer, a data processor shall conduct a self-assessment of the risks of the cross-border data transfer, focusing on the following:

(1) the legality, propriety, and necessity of the purpose, scope, and method of the cross-border data transfer by the data processor and the overseas recipient;



Source: https://www.danyoungcpa.com/cross-border-data-transfer-security-assessment-measures-english-translation/

(2) the scale, scope, type, and sensitivity of the data to be transferred outside the territory, and the risks that the cross-border data transfer may pose to national security, the public interest, or the lawful rights and interests of individuals or organizations;

(3) the responsibilities and obligations undertaken by the overseas recipient, and whether the management, technical measures, and capabilities for fulfilling such responsibilities and obligations can ensure the security of the data to be transferred outside the territory;

(4) the risks of the data being tampered with, destroyed, leaked, lost, transferred, or illegally obtained or illegally used after being transferred outside the territory and during subsequent processing, and whether channels for safeguarding personal information rights and interests are unobstructed;

(5) whether the data cross-border transfer contract or other legally binding document to be entered into with the overseas recipient (the "Legal Document") fully stipulates the data security protection responsibilities and obligations; and

(6) other matters that may affect the security of cross-border data transfer.

### Article 6

To apply for a security assessment of cross-border data transfer, the data processor shall submit the following materials to the national cyberspace administration authority through the local provincial-level cyberspace administration authority:

(1) an application form for the security assessment;

(2) the self-assessment report on the risks of the cross-border data transfer;

(3) the Legal Document to be entered into between the data processor and the overseas recipient;

(4) other materials necessary for the security assessment.

### Article 7

The provincial-level cyberspace administration authority shall complete the completeness check of the application materials within 5 working days of receiving them. If the materials are complete, they shall be submitted to the national cyberspace administration authority. If the materials are incomplete, the data processor shall be notified to supplement them.

### Article 8

The national cyberspace administration authority shall, within 7 working days of receiving the application materials from the provincial-level cyberspace administration authority, determine whether to accept the application and notify the data processor in writing. The security assessment shall be completed within 45 working days of the date when the national cyberspace administration authority issues a written notice of acceptance. Where the circumstances are complex or supplementary materials are required, the time limit may be appropriately extended, but the total processing time shall generally not exceed 60 working days.

### Article 9

When conducting a security assessment of cross-border data transfer, the national cyberspace administration authority shall focus on assessing the following:

(1) the legality, propriety, and necessity of the purpose, scope, and method of the cross-border data transfer;

(2) the impact of the data security protection policies, laws, and regulations of the country or region where the overseas recipient is located, and the cybersecurity environment, on the security of the data to be transferred outside the territory; whether the data protection level of the overseas recipient meets the requirements of the laws and administrative regulations of the People's Republic of China and the mandatory national standards;

(3) the scale, scope, type, and sensitivity of the data to be transferred outside the territory, and the risks that the cross-border data transfer may pose to national security, the public interest, or the lawful rights and interests of individuals or organizations;

(4) whether the data security protection responsibilities and obligations in the Legal Document between the data processor and the overseas recipient, as well as other legally binding documents it undertakes to comply with, are sufficiently stipulated;

(5) whether, after the data is transferred outside the territory, it will be at risk of being tampered with, destroyed, leaked, lost, transferred, or illegally obtained or illegally used;

(6) whether channels for safeguarding personal information rights and interests are unobstructed; and

(7) whether the provisions in the cross-border data transfer contract or other legal documents fully stipulate the data security protection responsibilities and obligations.

### Article 10

The national cyberspace administration authority shall, after accepting an application, organize relevant departments of the State Council, provincial-level cyberspace administration authorities, specialized institutions, and other relevant parties to conduct the security assessment of cross-border data transfer. Where it involves the responsibilities of relevant departments, the national cyberspace administration authority shall seek their opinions.

### Article 11

Upon completion of the security assessment, the national cyberspace administration authority shall make a decision in accordance with the law and notify the data processor of the assessment result in writing. The security assessment result shall be valid for 2 years from the date of issuance. Where the assessment concludes that the cross-border data transfer is not to be permitted, the data processor may not provide the data outside the territory.

### Article 12

Where any of the following circumstances occurs during the validity period of the security assessment result, the data processor shall reapply for a security assessment:

(1) the purpose, scope, method, or type of the cross-border data transfer, and the purpose and method of processing the data outside the territory by the overseas recipient change, affecting the security of the data transferred outside the territory, or the retention period of personal information and important data outside the territory is extended;

(2) the data security protection policies, laws, and regulations, and the cybersecurity environment of the country or region where the overseas recipient is located change, or other force majeure events occur, or the actual control of the data processor or the overseas recipient changes, or the Legal Document between the data processor and the overseas recipient is modified, which may affect the security of the data transferred outside the territory;

(3) other circumstances that affect the security of the data transferred outside the territory.

### Article 13

Where the national cyberspace administration authority discovers during the validity period of the security assessment result that the data processor has committed any act that affects the security of the data transferred outside the territory, or that the data transferred outside the territory is no longer secure, it shall revoke the assessment result in accordance with the law and notify the data processor in writing. The data processor shall cease the relevant cross-border data transfer activities.



Source: https://www.danyoungcpa.com/cross-border-data-transfer-security-assessment-measures-english-translation/

### Article 14

The data processor shall, within 10 working days after receiving the assessment result, submit the Legal Document entered into with the overseas recipient, the organizational and technical measures taken for data security protection, and other materials to the provincial-level cyberspace administration authority for filing.

### Article 15

After receiving the filing materials, the provincial-level cyberspace administration authority shall, within 10 working days, examine and verify the completeness of the materials. If the materials are complete and compliant, the authority shall issue a filing certificate. If the materials are incomplete or non-compliant, the data processor shall be notified to correct them.

### Article 16

Any organization or individual shall have the right to report to the national cyberspace administration authority or the provincial-level cyberspace administration authority any cross-border data transfer activity that violates the provisions of laws and administrative regulations. The authority receiving the report shall handle the matter in a timely manner in accordance with the law and inform the reporting party of the handling result.

### Article 17

Where a data processor violates these Measures by failing to apply for a security assessment of cross-border data transfer as required, or by providing data outside the territory without obtaining the security assessment result, the national cyberspace administration authority shall impose penalties in accordance with the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, and other applicable laws and administrative regulations.

### Article 18

Where the national cyberspace administration authority discovers that data that has already been transferred outside the territory poses a material risk to national security or the public interest during or after the assessment, it shall order the data processor to take corrective measures, including suspending the relevant cross-border data transfer activities, in accordance with the law.

### Article 19

For the purposes of these Measures:

(1) “Important data” means data that, if tampered with, destroyed, leaked, or illegally obtained or illegally used, may endanger national security, the operation of the economy, social stability, public health and safety, or other public interests.

(2) “Critical information infrastructure operator” means an operator designated as such in accordance with the Regulations on the Security Protection of Critical Information Infrastructure.

(3) “Cross-border data transfer” means the transfer of data collected and generated during operations within the territory of the People’s Republic of China, or stored within the territory, to recipients outside the territory.

### Article 20

These Measures shall come into force on September 1, 2022. Cross-border data transfer activities that have already been carried out before the implementation of these Measures shall complete corrective measures within 6 months of the implementation of these Measures if they fall within the scope of application of these Measures.

Disclaimer: This is an unofficial English translation provided for reference and informational purposes only. While every effort has been made to ensure accuracy, only the official Chinese version published by the National People's Congress (NPC) or the State Council of the People's Republic of China carries legal force. For legal matters, please consult a qualified professional. For official legal advice specific to your situation, contact Dan Young Business Consultancy.