

Measures for the Security Assessment of Data Exports of the PRC

Dan Young Business Consultancy — www.danyoungcpa.com

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

Issued by the Cyberspace Administration of China on July 7, 2022

Effective: September 1, 2022

Table of Contents

- Articles 1–20

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 laws and regulations for the purpose of regulating the security assessment of data exports, protecting personal information rights and interests, safeguarding national security and the public interest, and promoting the safe and free cross-border flow of data.

Article 2 — Where a data processor provides data collected and generated in the course of its operations within the territory of the People's Republic of China to an overseas recipient, a data export security assessment shall be conducted in accordance with these Measures. These Measures apply to the security assessment of data exports. The state shall, through data export security assessments, effectively prevent and control the risks to national security, the public interest, or the lawful rights and interests of individuals that may arise from data export.

Article 3 — The Cyberspace Administration of China shall be responsible for organizing and implementing data export security assessments. Before declaring for a data export security assessment, the data processor shall conduct a self-assessment of the data export risks in advance.

Article 4 — A data processor shall declare for a data export security assessment with the Cyberspace Administration of China through its local provincial-level cyberspace administration in any of the following circumstances: (1) exporting important data; (2) where a personal information processor that has processed the personal information of more than one million individuals provides personal information abroad; (3) where a personal information processor that has cumulatively provided abroad the personal information of more than 100,000 individuals or the sensitive personal information of more than 10,000 individuals since January 1 of the preceding year; or (4) other circumstances prescribed by the Cyberspace Administration of China that require a data export security assessment declaration.

Article 5 — The data processor shall submit the following materials when declaring for a data export security assessment: (1) the declaration letter; (2) the data export risk self-assessment report; (3) the legal document to be entered into between the data processor and the overseas recipient; and (4) other materials required for the security assessment. The legal document between the data processor and the overseas recipient shall specify the purpose, method, and scope of data export, the location and duration of data storage abroad, and the restrictive measures to be taken by the overseas recipient in the event of a change in the purpose or method of data processing.

Article 6 — The Cyberspace Administration of China shall, within seven working days from the date of receipt of the declaration materials, complete the review of completeness. Where the materials meet the requirements, a written notice of acceptance shall be issued. Where they do not meet the requirements, the data processor shall be notified to supplement or amend them.

Article 7 — The Cyberspace Administration of China shall complete the data export security assessment within 45 working days from the date of issuance of the written notice of acceptance. Where the circumstances are complex or supplementary materials are required, the assessment period may be appropriately extended, but the total assessment period shall generally not exceed 60 working days. The data processor shall not provide data abroad until the data export security assessment is completed.

Article 8 — The key items assessed in the data export security assessment include: (1) the legality, legitimacy, and necessity of the purpose, scope, and method of data export; (2) the impact of the data security protection policies and regulations of the country or region where the overseas recipient is located, and the cybersecurity environment, on the security of the exported data; (3) the data protection level of the overseas recipient and whether it meets the requirements of Chinese laws, administrative regulations, and mandatory national standards; (4) the scale, scope, type, and sensitivity of the data exported; (5) the risk of the exported data being tampered with, destroyed, divulged, lost, illegally obtained, or illegally used during or after export; and (6) whether the data security and personal information rights and interests can be fully and effectively protected.

Article 9 — The results of the data export security assessment shall be valid for two years from the date of issuance. Where a re-assessment is required due to a change in circumstances within the validity period, the data processor shall re-declare for assessment. During the validity period of the assessment results, where the Cyberspace Administration of China discovers that the data exported no longer meets the data export security requirements, it shall revoke the assessment results in writing and notify the data processor.

Article 10 — Data processors and their staff shall keep confidential any state secrets, personal privacy, personal information, trade secrets, confidential business information, and other information that comes to their knowledge in the course of performing their duties, and shall not divulge or illegally provide such information to others. Where a data processor violates the provisions of these Measures, punishment shall be imposed in accordance with the provisions of the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, and other laws and regulations.

Article 11 — These Measures shall come into force on September 1, 2022. These Measures shall apply to data export activities that have already been carried out before the effective date of these Measures but do not comply with the provisions of these Measures; the data processor shall complete the rectification within six months from the effective date of these Measures.

Disclaimer: This English translation is provided for reference and informational purposes only. While every effort has been made to ensure accuracy and completeness, this is not an official translation. The original Chinese text shall prevail as the authoritative version. Dan Young Business Consultancy makes no representations or warranties, express or implied, as to the accuracy, completeness, or suitability of this translation for any particular purpose. Readers should consult qualified legal professionals for advice on specific legal matters and refer to the official Chinese text for authoritative interpretation. Neither Dan Young Business Consultancy nor any of its affiliates shall be liable for any loss or damage arising from reliance on this translation.