Data Export Security Assessment Measures

Dan Young Business Consultancy — www.danyoungcpa.com

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

Contents

Table of Contents 1

Chapter I — General Provisions 1

Chapter II — Application for Security Assessment 2

Chapter III — Security Assessment Procedures 3

Chapter IV — Supervision and Administration 4

Chapter V — Supplementary Provisions 5

Table of Contents

- Chapter I — General Provisions
- Chapter II — Application for Security Assessment
- Chapter III — Security Assessment Procedures
- Chapter IV — Supervision and Administration
- Chapter V — Supplementary Provisions

Chapter I — General Provisions

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 relevant laws and regulations, for the purposes of regulating the security assessment of data export, protecting personal information rights and interests, safeguarding national security and the public interest, and promoting the safe and free flow of data across borders in accordance with the law.

Article 2 — These Measures apply to the security assessment of the provision abroad by data processors of important data and personal information collected and generated during operations within the territory of the People’s Republic of China.

Article 3 — The security assessment of data export shall adhere to the principles of combining pre-export assessment with ongoing supervision, and combining risk self-assessment with security assessment, to prevent the security risks that may arise from data export and ensure the orderly and free flow of data in accordance with the law.

Article 4 — Where a data processor provides data abroad, it shall file an application for a security assessment of data export with the national cyberspace administration authority through the local cyberspace administration authority at the provincial level in any of the following circumstances:

(1) A data processor provides important data abroad;

Source: https://www.danyoungcpa.com/data-export-security-assessment-measures-2022/

(2) A critical information infrastructure operator or a data processor processing personal information of more than one million individuals provides personal information abroad;

(3) A data processor that has provided personal information abroad cumulatively involving the personal information of 100,000 or more individuals, or the sensitive personal information of 10,000 or more individuals, since January 1 of the previous year; or

(4) Other circumstances where a security assessment of data export is required as prescribed by the national cyberspace administration authority.

Chapter II — Application for Security Assessment

Article 5 — Before filing an application for a security assessment of data export, a data processor shall conduct a self-assessment of the risks of data export, focusing on the following matters:

(1) The legality, propriety and necessity of the purpose, scope and method of the data export and of the data processing by the foreign recipient;

(2) The scale, scope, type and sensitivity of the data exported, and the risks that may be posed by the data export to national security, the public interest, or the lawful rights and interests of individuals or organizations;

(3) Whether the responsibilities and obligations undertaken by the foreign recipient, and the management, technical measures and capabilities for fulfilling such responsibilities and obligations, can ensure the security of the data exported;

(4) The risk of the data being tampered with, destroyed, disclosed, lost, transferred or illegally obtained or used after export, and whether channels for safeguarding personal information rights and interests are accessible;

(5) Whether the data export contract or other legally binding documents (hereinafter collectively referred to as “legal documents”) to be entered into with the foreign recipient fully specifies the responsibilities and obligations of each party for data security protection; and

(6) Other matters that may affect the security of the data export.

Article 6 — When filing an application for a security assessment of data export, the data processor shall submit the following materials:

(1) A written application;

(2) The self-assessment report on the risks of data export;

(3) The legal documents to be entered into by the data processor and the foreign recipient;

(4) Other materials required for the security assessment.

Article 7 — The local cyberspace administration authority at the provincial level shall, within five working days of receiving the application materials, complete the review of the completeness of the materials. Where the materials are complete, the application shall be submitted to the national cyberspace administration authority; where the materials are incomplete, the data processor shall be notified to supplement the materials in one go, and the data processor shall supplement the materials within the prescribed time limit.

Article 8 — The legal documents to be entered into by the data processor and the foreign recipient shall clearly specify the following content:

(1) The purpose, method and scope of the data export, and the purpose and method of the data processing by the foreign recipient;

Source: https://www.danyoungcpa.com/data-export-security-assessment-measures-2022/

(2) The place and time limit for storing the data abroad, and the measures for handling the data upon expiration of the storage period or upon completion of the agreed purpose;

(3) The restrictive provisions restricting the foreign recipient from transferring the exported data to other organizations or individuals;

(4) The security measures to be taken by the foreign recipient where there are any changes in its actual control or business scope, or where the laws, regulations and policies of the country or region where it is located that affect the performance of the data security protection obligations under the contract;

(5) The binding and enforceable provisions on the obligations of the foreign recipient to safeguard the rights and interests of personal information subjects;

(6) The remedial measures, liability for breach of contract, and dispute resolution methods for breach of the data security protection obligations; and

(7) Other obligations to be performed for data security protection.

Article 9 — The data processor shall be responsible for the authenticity of the materials submitted and shall not submit false materials or conceal relevant information.

Chapter III — Security Assessment Procedures

Article 10 — The national cyberspace administration authority shall, within seven working days of receiving the application materials, determine whether to accept the application and notify the data processor in writing.

Article 11 — After accepting a security assessment of data export, the national cyberspace administration authority shall, according to the circumstances of the application, organize the relevant departments of the State Council, the relevant provincial cyberspace administration authorities, specialized institutions, and industry experts to conduct the security assessment, focusing on the following matters:

(1) The legality, propriety and necessity of the purpose, scope and method of the data export;

(2) The impact of the data security protection policies, laws and regulations, and the network security environment of the country or region where the foreign recipient is located on the security of the data exported; and the extent to which the data protection level of the foreign 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 exported, and the risks of the data export to national security, the public interest, or the lawful rights and interests of individuals or organizations;

(4) Whether the personal information rights and interests of data subjects can be fully and effectively protected and whether channels exist for safeguarding such rights and interests;

(5) Whether the responsibilities and obligations of data security protection undertaken by the data processor and the foreign recipient in the relevant legal documents are comprehensive and adequate, and whether the corresponding management, technical measures and capabilities can prevent the risk of data being leaked or damaged;

(6) Other matters that need to be assessed.

Article 12 — The national cyberspace administration authority shall complete the security assessment of data export within 45 working days of the date of issuing the written notice of acceptance to the data processor; where the circumstances are complex or supplementary materials are required, the period may be appropriately extended and the data processor shall be notified of the expected extended period.

Source: https://www.danyoungcpa.com/data-export-security-assessment-measures-2022/

The time taken for the data processor to supplement or correct the materials shall not be counted within the assessment period specified in the preceding paragraph.

Article 13 — After completion of the security assessment of data export, the national cyberspace administration authority shall make a decision on the security assessment in accordance with the law and notify the data processor in writing. The security assessment result shall be valid for two years.

Where the security assessment result is that the data export is approved, the data processor may export data abroad during the validity period. Where the security assessment result is that the data export is not approved, the data processor shall not export data abroad.

Article 14 — During the validity period of the security assessment result, the data processor shall re-file an application for assessment in any of the following circumstances:

(1) The purpose, method, scope or type of the data export, and the purpose or method of the data processing by the foreign recipient have changed, or the retention period of the personal information and important data abroad has been extended;

(2) There are changes in the data security protection policies, laws and regulations, and the network security environment of the country or region where the foreign recipient is located, or there are other force majeure events that affect data security;

(3) There are changes in the actual control of the data processor or the foreign recipient, or there are changes in the legal documents between the data processor and the foreign recipient; or

(4) Other circumstances affecting the security of data export.

Where the validity period expires and it is necessary to continue the data export, the data processor shall re-file an application for assessment 60 working days prior to the expiration of the validity period.

Article 15 — During the validity period of the security assessment result, where the national cyberspace administration authority discovers that the data export no longer meets the security management requirements for data export, it shall revoke the security assessment result. The data processor shall terminate the data export upon receipt of the written notice of revocation.

Chapter IV — Supervision and Administration

Article 16 — The national cyberspace administration authority shall strengthen the supervision and administration of data export and establish a mechanism for the supervision and verification of the security management of data export.

The national cyberspace administration authority shall have the authority to conduct random inspections, verifications and on-site inspections of the data processor’s data export activities, and the data processor shall cooperate with such work.

Article 17 — Any organization or individual shall have the right to report to the national cyberspace administration authority a data processor’s failure to perform its data security protection obligations or any violation of the relevant provisions on the security management of data export.

The national cyberspace administration authority shall keep the identity of the reporter confidential and protect the lawful rights and interests of the reporter.

Article 18 — Where a data processor, in violation of these Measures, fails to perform its data security protection obligations, the national cyberspace administration authority shall handle the matter in accordance with the provisions of 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.

Source: https://www.danyoungcpa.com/data-export-security-assessment-measures-2022/

Chapter V — Supplementary Provisions

Article 19 — For the purposes of these Measures:

“Data export” means the provision by a data processor of data collected and generated during operations within the territory of the People’s Republic of China to organizations or individuals outside the territory, including:

(1) A data processor transfers or stores data abroad;

(2) Data collected and generated by a data processor is stored within the territory of the People’s Republic of China but can be accessed, retrieved, downloaded or exported by organizations or individuals abroad; and

(3) Other data export activities as prescribed by the national cyberspace administration authority.

Article 20 — These Measures shall take effect on September 1, 2022. Measures for the Security Assessment of Cross-Border Data Transfer that were implemented prior to the effective date of these Measures shall be repealed simultaneously.

Disclaimer: This English translation is provided for informational and reference purposes only. While every effort has been made to ensure accuracy, it is not an official translation and may contain differences from the original Chinese text. For legal purposes, the original Chinese version published by the Cyberspace Administration of China shall prevail. Dan Young Business Consultancy assumes no liability for any errors, omissions, or reliance on this translation. Users should consult qualified legal professionals for advice on specific matters relating to cross-border data transfer compliance in China.

Source: https://www.danyoungcpa.com/data-export-security-assessment-measures-2022/