Network Data Security Management Regulations

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 — General Obligations for Network Data Security 2

Chapter III — Protection of Personal Information 3

Chapter IV — Security of Important Data 4

Chapter V — Cross-Border Security Management of Network Data 5

Chapter VI — Obligations of Internet Platform Service Providers 5

Chapter VII — Supervision and Administration 6

Chapter VIII — Legal Liability 7

Chapter IX — Supplementary Provisions 8

Adopted at the 40th Executive Meeting of the State Council on August 30, 2024

Table of Contents

- Chapter I — General Provisions
- Chapter II — General Obligations for Network Data Security
- Chapter III — Protection of Personal Information
- Chapter IV — Security of Important Data
- Chapter V — Cross-Border Security Management of Network Data
- Chapter VI — Obligations of Internet Platform Service Providers
- Chapter VII — Supervision and Administration
- Chapter VIII — Legal Liability
- Chapter IX — Supplementary Provisions

Chapter I — General Provisions

Article 1 — These Regulations 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, for the purposes of regulating network data processing activities, safeguarding network data security, promoting the lawful, reasonable and

Source: https://www.danyoungcpa.com/network-data-security-management-regulations-2024/

effective use of network data, protecting the lawful rights and interests of individuals and organizations, and safeguarding national security and the public interest.

Article 2 — These Regulations apply to network data processing activities and the supervision and administration of network data security within the territory of the People's Republic of China.

Article 3 — Network data security management shall adhere to the overall concept of national security, uphold the leadership of the Communist Party of China, follow the principles of lawful administration, clear rights and responsibilities, coordination and cooperation, classified and graded management, and appropriate protection, and combine government supervision with industry self-discipline and social supervision.

Article 4 — The State shall encourage the development and application of network data security technologies, support the research, development and promotion of network data security products and services, promote the innovation and application of network data security technologies, and strengthen the cultivation of network data security professionals.

Article 5 — The State shall promote international exchanges and cooperation in the field of network data security, actively participate in the formulation of international rules and standards for network data security, and facilitate the secure and free flow of data across borders.

Article 6 — The national cyberspace administration authority shall be responsible for the overall planning and coordination of network data security management and the relevant supervision and administration work. The relevant departments of the State Council shall, in accordance with their respective duties, be responsible for the supervision and administration of network data security.

Relevant departments of local people's governments at or above the county level shall, in accordance with their respective duties, be responsible for the supervision and administration of network data security within their respective administrative regions.

Article 7 — Industry organizations shall, in accordance with their charters, strengthen industry self-discipline in network data security, formulate codes of conduct and standards for network data security, guide their members in strengthening network data security protection, raise the level of network data security protection, and promote the healthy development of the industry.

Article 8 — All entities and individuals shall have the right to report conduct that endangers network data security to the cyberspace administration authority and the relevant departments. The departments receiving such reports shall handle them in a timely manner in accordance with the law and keep the information of the reporters confidential.

Chapter II — General Obligations for Network Data Security

Article 9 — Network data processors shall, in accordance with the provisions of laws and administrative regulations and the mandatory requirements of national standards, establish and improve network data security management systems, adopt necessary security protection measures such as technical measures, and ensure the security of network data processing activities.

Article 10 — Network data processors shall designate a person responsible for network data security, establish a network data security management body, and specify the responsibilities of the person responsible for network data security and the network data security management body.

Article 11 — Network data processors shall provide network data security education and training for their employees, and enhance their employees' awareness and capability for network data security protection.

Article 12 — Network data processors shall, when processing network data, clearly specify the purpose, method and scope of processing, adhere to the principles of legality, propriety, necessity and good faith, and

Source: https://www.danyoungcpa.com/network-data-security-management-regulations-2024/

shall not process network data excessively.

Article 13 — Network data processors shall, in accordance with the provisions of laws and administrative regulations, adopt technical measures such as data classification and grading, encrypted transmission and storage, access control, and identity authentication to safeguard network data security.

Article 14 — Network data processors shall establish emergency response plans for network data security incidents. Where a network data security incident occurs, the network data processor shall immediately activate the emergency response plan, take remedial measures, promptly notify the users and report to the relevant competent authorities in accordance with the provisions.

Article 15 — Network data processors providing network products and services shall comply with the relevant provisions of the State, and where the network products and services involve the collection of users' information, the users shall be informed and their consent obtained. Network products and services that may pose a threat to national security shall pass a security review organized by the national cyberspace administration authority in conjunction with the relevant departments of the State Council.

Article 16 — Network data processors shall, when using automated decision-making technology, ensure the transparency of the decision-making and the fairness and impartiality of the results. Where automated decision-making is used to push information or provide commercial marketing to individuals, options not specific to their personal characteristics shall be provided, or convenient means of refusal shall be made available.

Article 17 — Network data processors shall retain network logs for not less than six months in accordance with the provisions of laws and administrative regulations.

Article 18 — Network data processors shall conduct regular security assessments of their network data processing activities, promptly identify and rectify security defects and vulnerabilities, and improve network data security protection measures.

Article 19 — Where network data processors entrust other parties to process network data, they shall enter into a written agreement with the entrusted party specifying the purpose, time limit, method, type of network data, and protection measures to be taken, and shall supervise the network data processing activities of the entrusted party.

Upon expiration of the entrustment period, the entrusted party shall return or delete the network data as agreed and shall not retain it without authorization.

Article 20 — Where network data processors share or transfer network data to other network data processors, they shall specify the purpose, method, and scope of the sharing or transfer, obtain consent in accordance with the law where necessary, and record the sharing or transfer.

Article 21 — Network data processors providing network data to foreign judicial or law enforcement authorities shall obtain the approval of the relevant competent authorities of the State Council.

Article 22 — Network data processors shall, upon termination or dissolution, promptly delete or anonymize the network data they have collected.

Article 23 — The State shall establish a catalogue of core network equipment, special-purpose cybersecurity products, and network critical equipment and special-purpose cybersecurity products for which security certification or security testing is mandatory, and shall implement security certification and security testing systems. No entity or individual may sell or provide network critical equipment and special-purpose cybersecurity products that have not passed security certification or security testing.

Chapter III — Protection of Personal Information

Source: https://www.danyoungcpa.com/network-data-security-management-regulations-2024/

Article 24 — Network data processors shall, when processing personal information, comply with the provisions of the Personal Information Protection Law of the People's Republic of China and relevant laws and administrative regulations.

Article 25 — Network data processors shall not collect personal information that is not necessary for the provision of services, shall not collect personal information by misleading, fraudulent or coercive means, and shall not collect personal information by bundling authorization or making repeated requests for authorization.

Article 26 — Network data processors shall, when collecting sensitive personal information, obtain the individual's separate consent and inform the individual of the necessity of collecting the sensitive personal information and the impact on the individual's rights and interests.

Article 27 — Network data processors shall provide individuals with convenient means of accessing, copying, correcting, supplementing, and deleting their personal information, and shall not set unreasonable conditions for individuals to exercise their rights.

Article 28 — Where network data processors transfer personal information abroad, they shall meet the conditions specified in Article 38 of the Personal Information Protection Law of the People's Republic of China and pass security assessments or obtain personal information protection certification or enter into standard contracts in accordance with the law.

Article 29 — Network data processors shall, when processing the personal information of minors under the age of 14, obtain the consent of their parents or other guardians and formulate specific personal information processing rules.

Article 30 — Network data processors shall designate a person responsible for personal information protection, publicly disclose their contact information, and report their name and contact information to the department performing personal information protection duties.

Chapter IV — Security of Important Data

Article 31 — The State shall implement a categorized and graded protection system for data. The national cyberspace administration authority shall, in conjunction with the relevant departments of the State Council, formulate catalogues of important data and strengthen the security protection of important data.

Article 32 — Network data processors shall determine the specific catalogue of important data within their respective organizations based on the catalogue of important data formulated by the State and the relevant identification guidelines, and shall report such catalogue to the relevant competent authorities for the record.

Article 33 — Network data processors processing important data shall specify the person responsible for data security and the management body, and implement security protection responsibilities for important data.

Article 34 — Network data processors shall, when processing important data, conduct risk assessments on their data processing activities on a regular basis and submit risk assessment reports to the relevant competent authorities.

The risk assessment shall include the following content:

(1) The type, quantity, scope, and method of processing of the important data;

(2) The security risks that may arise from the processing of important data and the impact on national security, the public interest, or the lawful rights and interests of individuals and organizations;

(3) The appropriateness of the security protection measures taken and the effectiveness of their implementation; and

Source: https://www.danyoungcpa.com/network-data-security-management-regulations-2024/

(4) Other matters that need to be assessed.

Article 35 — Network data processors processing important data shall, when merging, dividing, dissolving, or declaring bankruptcy, report to the relevant competent authorities in accordance with the provisions and handle the important data in a secure manner.

Article 36 — Network data processors providing important data abroad shall pass the security assessment for cross-border data transfer organized by the national cyberspace administration authority. Where laws, administrative regulations or the provisions of the national cyberspace administration authority provide otherwise, such provisions shall prevail.

Chapter V — Cross-Border Security Management of Network Data

Article 37 — The State shall establish a security management system for the cross-border transfer of data and regulate the cross-border transfer of data in accordance with the law. The cross-border security management of network data shall adhere to the principles of equal emphasis on data security and free flow of data, pre-transfer and ongoing supervision, and appropriate security assessment.

Article 38 — Where network data processors need to provide personal information and important data abroad for business purposes or other needs, they shall pass the security assessment for cross-border data transfer organized by the national cyberspace administration authority in accordance with the provisions, except as otherwise provided by laws, administrative regulations or the provisions of the national cyberspace administration authority.

Article 39 — Network data processors shall, when providing network data abroad, truthfully and completely declare the information on cross-border data transfer to the national cyberspace administration authority and submit relevant materials in accordance with the provisions. They shall not engage in false declarations or omissions or provide false materials.

Article 40 — Where the national cyberspace administration authority, after assessment, determines that cross-border data transfer may affect national security or harm the public interest, it shall not approve the cross-border data transfer.

Article 41 — Network data processors shall, after providing network data abroad, continue to fulfill their data security protection obligations and shall not transfer the risks of cross-border data security management to foreign recipients.

Article 42 — Network data processors providing network data abroad shall enter into contracts or other legally binding documents with the foreign recipients specifying the purpose, method and scope of the data transfer, the security protection measures to be taken, and the responsibilities and obligations of each party for data security protection.

Article 43 — Where there occur any changes in the purpose, method, or scope of cross-border data transfer, or any changes in the foreign recipient’s data security protection capability, or any changes in the laws, regulations, or policies of the country or region where the foreign recipient is located that may affect the security of the network data transferred, the network data processor shall promptly re-declare for a security assessment.

Chapter VI — Obligations of Internet Platform Service Providers

Article 44 — Internet platform service providers shall establish platform rules and privacy policies for network data security management, specifying the obligations of platform users for data security protection, the data security protection measures, and the rules for handling violations.

Article 45 — Internet platform service providers shall, in accordance with the provisions of laws and administrative regulations, verify and register the identity information of platform users and shall not provide

Source: https://www.danyoungcpa.com/network-data-security-management-regulations-2024/

services to users who refuse to provide their real identity information, except as otherwise provided by laws or administrative regulations.

Article 46 — Internet platform service providers shall establish a risk assessment mechanism for the platform's data security, and where data security risks are identified, they shall promptly take protective measures and report to the relevant competent authorities.

Article 47 — Internet platform service providers shall, when providing services to users by means of personalized recommendations, provide options not specific to the users' personal characteristics or provide convenient means of refusal to the users.

Article 48 — Internet platform service providers shall, when processing data by means of automated decision-making that has a significant impact on the rights and interests of users, ensure the transparency of the decision-making and the fairness and impartiality of the results, and provide users with channels for filing complaints.

Article 49 — Internet platform service providers that use personal information for automated decision-making to engage in differential pricing or other differential treatment shall not engage in unreasonable differential treatment of users under the same trading conditions.

Article 50 — Internet platform service providers providing services to a large number of users and having significant influence shall, in accordance with the provisions of the State, establish and improve an external oversight mechanism for network data security and make public the information on the performance of their network data security protection obligations.

Article 51 — Internet platform service providers shall cooperate with the supervision and inspection conducted by the national cyberspace administration authority and the relevant departments in accordance with the law and shall not refuse, obstruct, or evade such supervision and inspection.

Chapter VII — Supervision and Administration

Article 52 — The national cyberspace administration authority shall, in conjunction with the relevant departments of the State Council, establish a coordination mechanism for network data security management, strengthen the overall planning and coordination of network data security management, and coordinate and address major issues in network data security management.

Article 53 — The departments responsible for the supervision and administration of network data security shall, in accordance with the provisions of laws and administrative regulations, carry out supervision and inspection of network data security and have the authority to take the following measures:

(1) Review and copy the materials relating to network data processing;

(2) Make inquiries of the network data processor and the relevant personnel about the matters relating to network data processing;

(3) Conduct on-site inspections of the premises and facilities used for network data processing;

(4) Inspect and test the technical measures and equipment relating to network data security;

(5) Where there is evidence that network data processing activities endanger network data security or are suspected of violating laws, seal up or distrain the relevant equipment and facilities, or freeze the relevant network data; and

(6) Other measures as prescribed by laws and administrative regulations.

Article 54 — The departments responsible for the supervision and administration of network data security shall, when carrying out supervision and inspection, have at least two staff members present, produce their law enforcement credentials, and comply with the relevant provisions on law enforcement procedures.

Source: https://www.danyoungcpa.com/network-data-security-management-regulations-2024/

Staff members of the departments responsible for the supervision and administration of network data security shall keep confidential the personal information, personal privacy, trade secrets and other information that comes to their knowledge in the course of performing their duties and shall not disclose or illegally provide such information to others.

Article 55 — The national cyberspace administration authority shall, in conjunction with the relevant departments of the State Council, establish a credit record system for network data security and law-breaking and include the conduct of network data processors violating network data security laws and regulations in the credit records.

Article 56 — The State shall encourage social oversight of network data security and support industry organizations, media, and the public in carrying out oversight of network data security.

Chapter VIII — Legal Liability

Article 57 — Where a network data processor fails to perform the network data security protection obligations specified in these Regulations, the department performing network data security supervision and administration duties shall order it to make corrections and give it a warning, and may impose a fine of not less than 50,000 yuan but not more than 500,000 yuan; where the circumstances are serious, it may impose a fine of not less than 500,000 yuan but not more than 5,000,000 yuan, and may order the suspension of the relevant business, suspension of operations for rectification, or revocation of the relevant business permits or business licenses, and impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on the directly responsible person in charge and other directly responsible personnel.

Article 58 — Where a network data processor collects personal information in violation of the provisions of these Regulations, the department performing personal information protection duties shall order it to make corrections and give it a warning, confiscate its unlawful gains, and impose a fine of not more than 1,000,000 yuan on the network data processor; where the circumstances are serious, it shall order it to suspend or terminate the provision of services and impose a fine of not more than 50,000,000 yuan or a fine of not more than 5 percent of the previous year’s annual revenue, and impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on the directly responsible person in charge and other directly responsible personnel.

Article 59 — Where a network data processor provides important data abroad without passing a security assessment in violation of the provisions of these Regulations, the national cyberspace administration authority shall order it to make corrections and give it a warning, and may impose a fine of not less than 100,000 yuan but not more than 200,000 yuan; where the circumstances are serious, it may impose a fine of not less than 200,000 yuan but not more than 2,000,000 yuan, and may order the suspension of the relevant business, suspension of operations for rectification, or revocation of the relevant business permits or business licenses, and impose a fine of not less than 20,000 yuan but not more than 200,000 yuan on the directly responsible person in charge and other directly responsible personnel.

Article 60 — Where network data processors engage in false declarations, omissions, or the provision of false materials when providing network data abroad or during security assessments, the national cyberspace administration authority shall order them to make corrections and may impose a fine of not less than 50,000 yuan but not more than 100,000 yuan; where the circumstances are serious, it may impose a fine of not less than 100,000 yuan but not more than 1,000,000 yuan.

Article 61 — Where an internet platform service provider violates the provisions of Articles 44 through 51 of these Regulations, the national cyberspace administration authority and the relevant departments shall order it to make corrections and give it a warning in accordance with their respective duties; where the circumstances are serious, they shall impose a fine of not less than 100,000 yuan but not more than 1,000,000 yuan on the internet platform service provider and a fine of not less than 10,000 yuan but not more

Source: https://www.danyoungcpa.com/network-data-security-management-regulations-2024/

than 100,000 yuan on the directly responsible person in charge and other directly responsible personnel.

Article 62 — Where a network data processor, in violation of the provisions of these Regulations, causes damage to the lawful rights and interests of others, it shall bear civil liability in accordance with the law; where the violation constitutes a breach of public security administration, public security administration penalties shall be imposed in accordance with the law; where a crime is constituted, criminal liability shall be pursued in accordance with the law.

Article 63 — Where any staff member of a department responsible for the supervision and administration of network data security neglects their duties, abuses their powers, engages in malpractices for personal gain, or fails to keep confidential the personal information, trade secrets or other information that comes to their knowledge in the course of performing their duties, they shall be subject to sanctions in accordance with the law; where a crime is constituted, criminal liability shall be pursued in accordance with the law.

Chapter IX — Supplementary Provisions

Article 64 — These Regulations shall take effect on January 1, 2025.

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 promulgated by the State Council of the People's Republic 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 network data security compliance in China.

Source: https://www.danyoungcpa.com/network-data-security-management-regulations-2024/