Regulations on Network Data Security of the PRC

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 Rules 2

Chapter III — Protection of Personal Information 4

Chapter IV — Security of Important Data 6

Chapter V — Security Administration of Cross-Border Network Data 7

Chapter VI — Obligations of Network Platform Service Providers 8

Chapter VII — Supervision and Administration 9

Chapter VIII — Legal Liability 11

Chapter IX — Supplementary Provisions 12

Adopted at the 40th Executive Meeting of the State Council on August 30, 2024
Promulgated by Decree No. 790 of the State Council of the People's Republic of China on September 24, 2024
Effective: January 1, 2025

Table of Contents

- Chapter I — General Provisions
- Chapter II — General Rules
- Chapter III — Protection of Personal Information
- Chapter IV — Security of Important Data
- Chapter V — Security Administration of Cross-Border Network Data
- Chapter VI — Obligations of Network 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

Source: https://www.danyoungcpa.com/regulations-on-network-data-security-of-the-prc-2024/

Protection Law of the People's Republic of China, and other laws, for the purposes of regulating network data processing activities, safeguarding network data security, promoting the lawful, reasonable, and 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 carried out within the territory of the People's Republic of China and to the security supervision and administration thereof.

Activities processing the personal information of natural persons within the territory of the People's Republic of China from outside the territory, where the circumstances set out in paragraph 2 of Article 3 of the Personal Information Protection Law of the People's Republic of China are met, shall also be governed by these Regulations.

Where network data processing activities carried out outside the territory of the People's Republic of China harm the national security or public interest of the People's Republic of China or the lawful rights and interests of its citizens or organizations, legal liability shall be pursued in accordance with the law.

Article 3 — Network data security administration work shall uphold the leadership of the Communist Party of China, implement a holistic approach to national security, and coordinate the promotion of the development and utilization of network data and the safeguarding of network data security.

Article 4 — The state encourages the innovative application of network data in all industries and fields, strengthens the building of network data security protection capabilities, supports innovation in network data-related technologies, products, and services, carries out publicity and education on network data security and personnel training, and promotes the development, utilization, and industrial development of network data.

Article 5 — The state shall implement classified and graded protection of network data based on the degree of importance of network data in economic and social development and the degree of harm that would be caused to national security, the public interest, or the lawful rights and interests of individuals and organizations if such data were tampered with, destroyed, leaked, or illegally obtained or illegally used.

Article 6 — The state actively participates in the formulation of international rules and standards related to network data security and promotes international exchange and cooperation.

Article 7 — The state supports relevant industry organizations in formulating codes of conduct for network data security in accordance with their charters, strengthening industry self-discipline, guiding members to strengthen network data security protection, raising the level of network data security protection, and promoting the sound development of the industry.

Chapter II — General Rules

Article 8 — No individual or organization may use network data to engage in illegal activities, or engage in illegal network data processing activities such as stealing or otherwise illegally obtaining network data, or illegally selling or illegally providing network data to others.

No individual or organization may provide programs or tools specifically used for engaging in the illegal activities mentioned in the preceding paragraph; anyone who knows that others are engaging in the illegal activities mentioned in the preceding paragraph shall not provide them with technical support such as internet access, server hosting, network storage, or communication transmission, or provide assistance such as advertising promotion or payment settlement.

Article 9 — Network data processors shall, in accordance with the provisions of laws and administrative regulations and the mandatory requirements of national standards, and on the basis of graded protection of cybersecurity, strengthen network data security protection, establish and improve network data security management systems, adopt technical measures such as encryption, backup, access control, and security

Source: https://www.danyoungcpa.com/regulations-on-network-data-security-of-the-prc-2024/

certification and other necessary measures, protect network data from being tampered with, destroyed, leaked, or illegally obtained or illegally used, handle network data security incidents, guard against illegal and criminal activities carried out against or through the use of network data, and bear primary responsibility for the security of the network data they process.

Article 10 — Network products and services provided by network data processors shall conform to the mandatory requirements of relevant national standards; upon discovering security defects, vulnerabilities, or other risks in network products or services, they shall immediately take remedial measures, promptly notify users in accordance with regulations, and report to the competent departments; where national security or the public interest is endangered, network data processors shall also report to the competent departments within 24 hours.

Article 11 — Network data processors shall establish and improve contingency plans for network data security incidents. Upon the occurrence of a network data security incident, they shall immediately activate the contingency plan, take measures to prevent the expansion of harm, eliminate potential safety hazards, and report to the competent departments in accordance with regulations.

Where a network data security incident harms the lawful rights and interests of individuals or organizations, the network data processor shall promptly notify the interested persons of the security incident and risk situation, the harmful consequences, and the remedial measures already taken, by means such as telephone, short message, instant messaging tools, email, or public notice; where laws or administrative regulations provide that notification may be omitted, such provisions shall prevail. Where a network data processor, in the course of handling a network data security incident, discovers leads that are suspected of constituting illegal or criminal activity, it shall report to the public security organs or state security organs in accordance with regulations and cooperate in the investigation, inquiry, and handling work.

Article 12 — Where a network data processor provides personal information and important data to other network data processors or entrusts the processing thereof to others, it shall agree with the network data recipients, through contracts or otherwise, on the purposes, methods, and scope of processing and the security protection obligations, and shall supervise the recipients' performance of their obligations. Records of the processing of personal information and important data that are provided to or entrusted to other network data processors for processing shall be kept for at least 3 years.

Network data recipients shall perform network data security protection obligations and process personal information and important data in accordance with the agreed purposes, methods, scope, and the like.

Where two or more network data processors jointly determine the purposes and methods of processing personal information and important data, they shall agree on their respective rights and obligations.

Article 13 — Where network data processing activities carried out by a network data processor affect or may affect national security, a national security review shall be conducted in accordance with relevant state regulations.

Article 14 — Where a network data processor needs to transfer network data due to merger, division, dissolution, bankruptcy, or other reasons, the network data recipient shall continue to perform network data security protection obligations.

Article 15 — Where a state organ entrusts others to build, operate, or maintain an e-government system, or to store or process government data, it shall undergo strict approval procedures in accordance with relevant state regulations, specify the entrusted party's network data processing authority, protection responsibilities, and the like, and supervise the entrusted party's performance of network data security protection obligations.

Article 16 — Network data processors that provide services to state organs or critical information infrastructure operators, or that participate in the building, operation, or maintenance of other public infrastructure or public service systems, shall perform network data security protection obligations in

accordance with the provisions of laws and regulations and the stipulations of contracts, and provide secure, stable, and continuous services.

Network data processors specified in the preceding paragraph shall not, without the consent of the commissioning party, access, obtain, retain, use, disclose, or provide network data to others, or conduct correlation analysis of network data.

Article 17 — Information systems providing services for state organs shall strengthen network data security administration with reference to the administration requirements for e-government systems, to safeguard network data security.

Article 18 — Where a network data processor uses automated tools to access or collect network data, it shall assess the impact on network services, and shall not unlawfully intrude into others' networks or interfere with the normal operation of network services.

Article 19 — Network data processors providing generative artificial intelligence services shall strengthen security administration of training data and training data processing activities and take effective measures to prevent and handle network data security risks.

Article 20 — Network data processors that provide products or services to the public shall accept public supervision, establish convenient channels for complaints and reports concerning network data security, publish information such as the means of complaint and report, and promptly accept and handle complaints and reports concerning network data security.

Chapter III — Protection of Personal Information

Article 21 — Where, before processing personal information, a network data processor notifies individuals in accordance with the law by formulating rules for personal information processing, such rules shall be displayed publicly in a centralized manner, be easily accessible, and be placed in a conspicuous position, with clear, specific, and easily understandable content, including but not limited to the following:

(1) the name of the network data processor and its contact information;

(2) the purposes, methods, and types of processing personal information, the necessity of processing sensitive personal information, and the impact on the rights and interests of individuals;

(3) the retention period for personal information and the manner of handling after expiration; where the retention period is difficult to determine, the method for determining the retention period shall be specified;

(4) the methods and channels for individuals to consult, copy, transfer, correct, supplement, delete, and restrict the processing of their personal information, and to cancel accounts and withdraw consent.

Where a network data processor notifies individuals of the purposes, methods, and types of collecting personal information and of providing personal information to other network data processors, and the information of the network data recipients, in accordance with the preceding paragraph, it shall list such matters in the form of lists or otherwise. Where a network data processor processes the personal information of minors under the age of 14, it shall also formulate special rules for personal information processing.

Article 22 — Where a network data processor processes personal information based on the individual's consent, it shall comply with the following provisions:

(1) collection of personal information shall be necessary for the provision of products or services; personal information shall not be collected beyond the necessary scope; and consent shall not be obtained through misleading, fraudulent, or coercive means;

(2) where sensitive personal information such as biometric information, religious beliefs, specific identity, medical and health information, financial accounts, and whereabouts and tracks is processed, separate

Source: https://www.danyoungcpa.com/regulations-on-network-data-security-of-the-prc-2024/

consent shall be obtained from the individual;

(3) where the personal information of minors under the age of 14 is processed, consent shall be obtained from the minor's parents or other guardians;

(4) personal information shall not be processed beyond the purposes, methods, types, and retention period of processing to which the individual has consented;

(5) consent shall not be solicited frequently after the individual has expressly indicated disagreement with the processing of their personal information;

(6) where the purposes, methods, or types of processing personal information change, consent shall be obtained anew from the individual.

Where laws or administrative regulations provide that processing sensitive personal information requires written consent, such provisions shall prevail.

Article 23 — Where an individual requests to consult, copy, correct, supplement, delete, or restrict the processing of their personal information, or cancels an account or withdraws consent, the network data processor shall handle the request in a timely manner and provide convenient methods and channels supporting the individual's exercise of their rights, and shall not set unreasonable conditions to restrict the individual's reasonable requests.

Article 24 — Where collection of non-essential personal information, or personal information obtained without lawful consent, cannot be avoided due to the use of automated collection technologies or other reasons, or where an individual cancels an account, the network data processor shall delete the personal information or carry out anonymization processing. Where the retention period provided for by laws or administrative regulations has not expired, or deletion or anonymization of personal information is technically difficult to achieve, the network data processor shall cease processing other than storage and the adoption of necessary security protection measures.

Article 25 — With respect to a personal information transfer request that satisfies the following conditions, the network data processor shall provide channels for other network data processors designated by the individual to access and obtain the relevant personal information:

(1) the true identity of the requester can be verified;

(2) the personal information requested to be transferred was provided with the individual's consent or collected on the basis of a contract;

(3) the transfer of personal information is technically feasible;

(4) the transfer of personal information does not harm the lawful rights and interests of others.

Where the frequency of requests to transfer personal information or the like clearly exceeds a reasonable scope, the network data processor may charge necessary fees based on the cost of transferring the personal information.

Article 26 — Where a network data processor outside the territory of the People's Republic of China processes the personal information of natural persons within the territory and, in accordance with Article 53 of the Personal Information Protection Law of the People's Republic of China, establishes a dedicated agency within the territory or designates a representative, it shall report the name of the relevant agency or the name and contact information of the representative to the cyberspace administration department at the level of a city divided into districts where it is located; the cyberspace administration department shall promptly notify the competent departments at the corresponding level.

Article 27 — Network data processors shall regularly conduct compliance audits, by themselves or by entrusting professional institutions, of their compliance with laws and administrative regulations in processing

Source: https://www.danyoungcpa.com/regulations-on-network-data-security-of-the-prc-2024/

personal information.

Article 28 — Network data processors processing personal information of more than 10 million persons shall also comply with the provisions made in Articles 30 and 32 of these Regulations for network data processors processing important data (hereinafter referred to as "processors of important data").

Chapter IV — Security of Important Data

Article 29 — The national data security coordination mechanism shall coordinate relevant departments in formulating catalogs of important data and strengthen the protection of important data. All regions and departments shall, in accordance with the classified and graded data protection system, determine specific catalogs of important data in their respective regions and departments and relevant industries and fields, and carry out key protection of network data listed in the catalogs.

Network data processors shall, in accordance with relevant state regulations, identify and declare important data. Where data is confirmed as important data, the relevant regions and departments shall promptly notify the network data processors or make it public. Network data processors shall perform network data security protection responsibilities.

The state encourages network data processors to use technologies and products such as data labels to raise the level of important data security administration.

Article 30 — Processors of important data shall designate a person responsible for network data security and an institution for network data security administration. The institution for network data security administration shall perform the following network data security protection responsibilities:

(1) formulating and implementing network data security management systems, operating procedures, and contingency plans for network data security incidents;

(2) regularly organizing activities such as network data security risk monitoring, risk assessment, emergency drills, and publicity, education, and training, and promptly handling network data security risks and incidents;

(3) accepting and handling complaints and reports concerning network data security.

The person responsible for network data security shall possess professional knowledge of network data security and relevant management work experience, shall be a member of the management of the network data processor, and shall have the right to report network data security situations directly to the competent departments.

Network data processors that handle important data of specific types and scales prescribed by the competent departments shall conduct security background reviews of the person responsible for network data security and personnel in key positions, and strengthen training of relevant personnel. During the review, they may apply to the public security organs or state security organs for assistance.

Article 31 — Before providing, entrusting the processing of, or jointly processing important data, processors of important data shall conduct a risk assessment, except where it is performed in fulfillment of statutory duties or statutory obligations.

The risk assessment shall focus on assessing the following:

(1) whether the purposes, methods, and scope of providing, entrusting the processing of, or jointly processing network data, and of the network data recipients' processing of network data, are lawful, legitimate, and necessary;

(2) the risk that the network data provided, entrusted for processing, or jointly processed will be tampered with, destroyed, leaked, or illegally obtained or illegally used, and the risk to national security, the public interest, or the lawful rights and interests of individuals or organizations;

Source: https://www.danyoungcpa.com/regulations-on-network-data-security-of-the-prc-2024/

(3) the integrity, law-abiding conduct, and other circumstances of the network data recipients;

(4) whether the requirements on network data security in relevant contracts concluded or to be concluded with the network data recipients can effectively bind the network data recipients to perform network data security protection obligations;

(5) whether the technical and administrative measures adopted or to be adopted can effectively guard against risks such as network data being tampered with, destroyed, leaked, or illegally obtained or illegally used;

(6) other assessment content prescribed by the competent departments.

Article 32 — Where a processor of important data may affect important data security due to merger, division, dissolution, bankruptcy, or other reasons, it shall take measures to safeguard network data security and report to the competent departments at or above the provincial level the important data disposal plan, and the name and contact information of the recipient; where the competent department is unclear, it shall report to the data security coordination mechanism at or above the provincial level.

Article 33 — Processors of important data shall conduct an annual risk assessment of their network data processing activities and submit a risk assessment report to the competent departments at or above the provincial level; the competent departments shall promptly notify the cyberspace administration departments and public security organs at the corresponding level.

The risk assessment report shall include the following:

(1) the basic information of the network data processor, the information of the network data security administration institution, and the name and contact information of the person responsible for network data security;

(2) the purposes, types, quantity, methods, scope, storage period, and storage location of processing important data, and the state of carrying out network data processing activities, excluding the content of the network data itself;

(3) the network data security management systems and their implementation, and technical measures such as encryption, backup, labels, access control, and security certification and other necessary measures and their effectiveness;

(4) network data security risks discovered, and network data security incidents that occurred and their handling;

(5) the risk assessment of providing, entrusting the processing of, and jointly processing important data;

(6) the cross-border transfer of network data;

(7) other report content prescribed by the competent departments.

Risk assessment reports submitted by large online platform service providers processing important data shall, in addition to the content specified in the preceding paragraph, fully explain the network data security of key business and supply chains.

Where a processor of important data engages in important data processing activities that may endanger national security, the competent departments at or above the provincial level shall order it to take measures such as rectification or cessation of processing of important data. Processors of important data shall immediately take measures in accordance with the relevant requirements.

Chapter V — Security Administration of Cross-Border Network Data

Article 34 — The national cyberspace administration department shall coordinate relevant departments in establishing a national special working mechanism for the security administration of outbound data transfer,

research and formulate national policies on the security administration of outbound transfer of network data, and coordinate the handling of major matters concerning the security of outbound network data transfer.

Article 35 — Where any of the following conditions is met, network data processors may provide personal information overseas:

(1) passing the security assessment of outbound data transfer organized by the national cyberspace administration department;

(2) obtaining personal information protection certification by professional institutions in accordance with the provisions of the national cyberspace administration department;

(3) conforming to the provisions of the standard contract for outbound transfer of personal information formulated by the national cyberspace administration department;

(4) where it is truly necessary to provide personal information overseas for the conclusion or performance of a contract to which the individual is a party;

(5) where it is truly necessary to provide employees' personal information overseas for cross-border human resources administration implemented in accordance with labor rules formulated in accordance with the law and collective contracts concluded in accordance with the law;

(6) where it is truly necessary to provide personal information overseas for the performance of statutory duties or statutory obligations;

(7) where it is truly necessary to provide personal information overseas in emergency circumstances to protect the life, health, and property safety of natural persons;

(8) other conditions provided for by laws, administrative regulations, or the national cyberspace administration department.

Article 36 — Where international treaties or agreements concluded or acceded to by the People's Republic of China provide for the conditions for providing personal information overseas, they may be implemented in accordance with such provisions.

Article 37 — Where important data collected and generated by network data processors in their operations within the territory of the People's Republic of China truly needs to be provided overseas, it shall undergo the security assessment of outbound data transfer organized by the national cyberspace administration department. Where a network data processor has identified and declared important data in accordance with relevant state regulations but has not been notified by the relevant regions or departments, nor has such data been publicly released as important data, it is not required to declare such data as important data for security assessment of outbound data transfer.

Article 38 — After passing the security assessment of outbound data transfer, where a network data processor provides personal information and important data overseas, it shall not exceed the purposes, methods, scope, types, scale, and the like of outbound data transfer specified in the assessment.

Article 39 — The state shall take measures to guard against and handle cross-border network data security risks and threats. No individual or organization may provide programs or tools specifically used for destroying or circumventing technical measures; anyone who knows that others are engaging in activities such as destroying or circumventing technical measures shall not provide them with technical support or assistance.

Chapter VI — Obligations of Network Platform Service Providers

Article 40 — Network platform service providers shall, through platform rules or contracts, specify the network data security protection obligations of third-party product and service providers connected to their

Source: https://www.danyoungcpa.com/regulations-on-network-data-security-of-the-prc-2024/

platforms, and urge third-party product and service providers to strengthen network data security administration.

Producers of smart terminal devices and other equipment with pre-installed applications shall be governed by the preceding paragraph.

Where third-party product and service providers engage in network data processing activities in violation of the provisions of laws and administrative regulations, platform rules, or contractual stipulations, causing damage to users, the network platform service providers, the third-party product and service providers, and the producers of smart terminal devices and other equipment with pre-installed applications shall bear corresponding liability in accordance with the law.

The state encourages insurance companies to develop insurance products for network data damage liability, and encourages network platform service providers and producers of smart terminal devices and other equipment with pre-installed applications to purchase such insurance.

Article 41 — Network platform service providers providing application distribution services shall establish application verification rules and carry out verification related to network data security. Where applications to be distributed or already distributed are found not to conform to the provisions of laws and administrative regulations or the mandatory requirements of national standards, measures such as warning, refusing distribution, suspending distribution, or terminating distribution shall be taken.

Article 42 — Where a network platform service provider pushes information to individuals through automated decision-making, it shall set up an easily understandable, accessible, and operable option for closing personalized recommendations, and provide users with functions such as refusing to receive pushed information and deleting user tags based on their personal characteristics.

Article 43 — The state shall promote the building of public services for network identity authentication, and promote their application in accordance with the principles of government guidance and user voluntariness.

Network platform service providers are encouraged to support users in registering and verifying their true identity information through the public services for national network identity authentication.

Article 44 — Large network platform service providers shall publish an annual social responsibility report on personal information protection. The report shall include, but is not limited to, personal information protection measures and their results, the acceptance and handling of applications by individuals to exercise their rights, and the performance of duties by the personal information protection supervisory institution composed mainly of external members.

Article 45 — Large network platform service providers providing network data cross-border shall comply with national requirements on cross-border data security administration, improve relevant technical and administrative measures, and guard against cross-border network data security risks.

Article 46 — Large network platform service providers shall not use network data, algorithms, platform rules, and the like to engage in the following activities:

(1) processing network data generated by users on the platform through misleading, fraudulent, coercive, or other means;

(2) restricting, without legitimate reasons, users' access to and use of network data generated by them on the platform;

(3) imposing unreasonable differential treatment on users, harming users' lawful rights and interests;

(4) other activities prohibited by laws and administrative regulations.

Chapter VII — Supervision and Administration

Source: https://www.danyoungcpa.com/regulations-on-network-data-security-of-the-prc-2024/

Article 47 — The national cyberspace administration department shall be responsible for coordinating network data security and related supervision and administration work.

The public security organs and state security organs shall, in accordance with the provisions of relevant laws and administrative regulations and these Regulations, assume network data security supervision and administration duties within their respective scope of duties, and guard against and combat, in accordance with the law, illegal and criminal activities endangering network data security.

The national data administration department shall perform corresponding network data security duties in specifically undertaking data administration work.

All regions and departments shall be responsible for the network data collected and generated in their work and for network data security.

Article 48 — The relevant competent departments shall assume network data security supervision and administration duties in their respective industries and fields, designate institutions for network data security protection work in their industries and fields, formulate and organize the implementation of contingency plans for network data security incidents in their industries and fields, regularly organize network data security risk assessments in their industries and fields, supervise and inspect network data processors' performance of network data security protection obligations, and guide and urge network data processors to promptly rectify existing risks and hidden dangers.

Article 49 — The national cyberspace administration department shall coordinate the relevant competent departments in promptly aggregating, assessing, sharing, and publishing information related to network data security risks, and strengthen the sharing of network data security information, the monitoring and early warning of network data security risks and threats, and the emergency handling of network data security incidents.

Article 50 — The relevant competent departments may take the following measures to supervise and inspect network data security:

(1) requiring network data processors and their relevant personnel to explain matters subject to supervision and inspection;

(2) consulting and copying documents and records related to network data security;

(3) inspecting the operation of network data security measures;

(4) inspecting equipment and items related to network data processing activities;

(5) other necessary measures provided for by laws and administrative regulations.

Network data processors shall cooperate with the network data security supervision and inspection lawfully conducted by the relevant competent departments.

Article 51 — The relevant competent departments shall conduct network data security supervision and inspection objectively and impartially, and shall not charge fees to the units under inspection.

The relevant competent departments shall not, in network data security supervision and inspection, access or collect business information unrelated to network data security; the information obtained may be used only for the needs of safeguarding network data security and shall not be used for other purposes.

Where the relevant competent departments discover that a network data processor's network data processing activities present relatively significant security risks, they may, in accordance with the prescribed authority and procedures, require the network data processor to suspend relevant services, modify platform rules, improve technical measures, and the like, to eliminate network data security hazards.

Article 52 — In conducting network data security supervision and inspection, the relevant competent departments shall strengthen coordination, cooperation, and information communication, reasonably determine the frequency and methods of inspection, and avoid unnecessary inspections and overlapping or duplicate inspections.

Personal information protection compliance audits, risk assessments of important data, and security assessments of outbound transfer of important data shall be better connected to avoid duplicate assessment and auditing. Where the content of important data risk assessments and cybersecurity graded protection assessments overlaps, the relevant results may be mutually accepted.

Article 53 — The relevant competent departments and their staff shall, in accordance with the law, keep confidential network data such as personal privacy, personal information, trade secrets, and confidential business information that come to their knowledge in the performance of their duties, and shall not disclose or illegally provide them to others.

Article 54 — Where overseas organizations or individuals engage in network data processing activities that endanger the national security or public interest of the People's Republic of China, or infringe upon the personal information rights and interests of citizens of the People's Republic of China, the national cyberspace administration department, together with the relevant competent departments, may take corresponding necessary measures in accordance with the law.

Chapter VIII — Legal Liability

Article 55 — Where the provisions of Article 12, Articles 16 through 20, Article 22, paragraphs 1 and 2 of Article 40, Article 41, or Article 42 of these Regulations are violated, the cyberspace administration, telecommunications, public security, and other competent departments shall, in accordance with their respective duties, order correction, give a warning, and confiscate illegal gains; where correction is refused or the circumstances are serious, a fine of not more than 1 million yuan shall be imposed, and the suspension of relevant business, suspension of business for rectification, revocation of relevant business permits, or revocation of the business license may be ordered, and a fine of not less than 10,000 yuan but not more than 100,000 yuan may be imposed on the directly responsible persons in charge and other directly responsible personnel.

Article 56 — Where the provisions of Article 13 of these Regulations are violated, the cyberspace administration, telecommunications, public security, state security, and other competent departments shall, in accordance with their respective duties, order correction and give a warning, and may also impose a fine of not less than 100,000 yuan but not more than 1 million yuan, and may impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on the directly responsible persons in charge and other directly responsible personnel; where correction is refused or the circumstances are serious, a fine of not less than 1 million yuan but not more than 10 million yuan shall be imposed, and the suspension of relevant business, suspension of business for rectification, revocation of relevant business permits, or revocation of the business license may be ordered, and a fine of not less than 100,000 yuan but not more than 1 million yuan shall be imposed on the directly responsible persons in charge and other directly responsible personnel.

Article 57 — Where the provisions of paragraph 2 of Article 29, paragraphs 2 and 3 of Article 30, Article 31, or Article 32 of these Regulations are violated, the cyberspace administration, telecommunications, public security, and other competent departments shall, in accordance with their respective duties, order correction and give a warning, and may also impose a fine of not less than 50,000 yuan but not more than 500,000 yuan, and may impose a fine of not less than 10,000 yuan but not more than 100,000 yuan on the directly responsible persons in charge and other directly responsible personnel; where correction is refused or serious consequences such as the leakage of large quantities of data are caused, a fine of not less than 500,000 yuan but not more than 2 million yuan shall be imposed, and the suspension of relevant business, suspension of business for rectification, revocation of relevant business permits, or revocation of the

Source: https://www.danyoungcpa.com/regulations-on-network-data-security-of-the-prc-2024/

business license may be ordered, and a fine of not less than 50,000 yuan but not more than 200,000 yuan shall be imposed on the directly responsible persons in charge and other directly responsible personnel.

Article 58 — Where other relevant provisions of these Regulations are violated, the relevant competent departments shall pursue legal liability in accordance with the relevant 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.

Article 59 — Where a network data processor has circumstances such as proactively eliminating or mitigating the harmful consequences of an illegal act, committing a minor illegal act and promptly correcting it without causing harmful consequences, or committing an illegal act for the first time with minor harmful consequences and promptly correcting it, it shall be given a lighter or mitigated administrative penalty or be exempted from administrative penalty in accordance with the provisions of the Administrative Penalty Law of the People's Republic of China.

Article 60 — Where a state organ fails to perform its network data security protection obligations under these Regulations, its higher-level organ or the relevant competent department shall order correction; the directly responsible persons in charge and other directly responsible personnel shall be given sanctions in accordance with the law.

Article 61 — Where a violation of these Regulations causes damage to others, civil liability shall be borne in accordance with the law; where it constitutes a violation of public security administration, public security administration penalties shall be imposed in accordance with the law; where it constitutes a crime, criminal liability shall be pursued in accordance with the law.

Chapter IX — Supplementary Provisions

Article 62 — For the purposes of these Regulations, the following terms shall have the following meanings:

(1) "network data" means all kinds of electronic data processed and generated through networks;

(2) "network data processing activities" means activities such as the collection, storage, use, processing, transmission, provision, disclosure, and deletion of network data;

(3) "network data processor" means an individual or organization that autonomously determines the purposes and methods of processing in network data processing activities;

(4) "important data" means data that, in specific fields, for specific groups, in specific regions, or reaching a certain precision and scale, once tampered with, destroyed, leaked, or illegally obtained or illegally used, may directly endanger national security, economic operation, social stability, or public health and safety;

(5) "entrusted processing" means network data processing activities carried out by an individual or organization entrusted by a network data processor in accordance with the agreed purposes and methods;

(6) "joint processing" means network data processing activities in which two or more network data processors jointly determine the purposes and methods of processing network data;

(7) "separate consent" means specific and clear consent given by an individual specifically for a particular processing of their personal information;

(8) "large network platform" means a network platform with more than 50 million registered users or more than 10 million monthly active users, with complex business types, whose network data processing activities have an important impact on national security, economic operation, the national economy, and people's livelihood.

Article 63 — Network data processing activities involving core data shall be carried out in accordance with relevant state regulations.

Source: https://www.danyoungcpa.com/regulations-on-network-data-security-of-the-prc-2024/

These Regulations do not apply to natural persons processing personal information for personal or family affairs.

Network data processing activities involving state secrets or work secrets shall be governed by the provisions of the Law of the People's Republic of China on Guarding State Secrets and other laws and administrative regulations.

Article 64 — These Regulations shall come into force on January 1, 2025.

Disclaimer: This is an unofficial English translation of the original Chinese text, prepared for reference and informational purposes only. It is not an official translation and has no legal effect. In the event of any discrepancy between this translation and the original Chinese text, the original Chinese text shall prevail. For legal or business decisions, please refer to the official Chinese version or seek professional legal advice.