

本译文仅供学习交流，不得用于任何商业用途

**The English translation below is for information only
and may not be reproduced or otherwise used for any
commercial purpose.**

Decree of the State Council of the People's Republic of China
No.790

The Regulations on Network Data Security Management, adopted at the 40th Executive Meeting of the State Council on August 30, 2024, are hereby promulgated and shall be effective as of January 1, 2025.

Premier Li Qiang
September 24, 2024

Regulations on Network Data Security Management

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, ensuring the security of network data, promoting the reasonable and effective use of network data in accordance with the law, protecting the legitimate rights and interests of individuals and organizations, and safeguarding national security and public interests.

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

These Regulations also apply to the activities conducted outside the territory of the People's Republic of China that process the personal information of natural persons within the territory of the People's Republic of China, provided that such activities fall under the circumstances specified in paragraph 2 of Article 3 of the Personal Information Protection Law of the People's Republic of China.

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

Article 3 The management of network data security shall adhere to the leadership of the Communist Party of China, implement the holistic approach to national security, and coordinate the promotion of network data development and utilization with the assurance of network data security.

Article 4 The State encourages the innovative application of network data in all industries and sectors, strengthens the construction of network data security protection capabilities, supports innovation in technologies, products, and services related to network data, carries out publicity, education, and talent cultivation for network data security, and promotes the development, utilization, and industrial growth of network data.

Article 5 The State implements categorized and classified protection for network data based on the importance of the data in economic and social development and the extent of harm caused to national security, public interests, or the legitimate rights and interests of individuals or organizations in the event of its alteration, destruction, leakage, or illegal acquisition or utilization.

Article 6 The State actively engages in the formulation of international rules and standards related to network data security to promote international exchange and cooperation.

Article 7 The State supports relevant industry associations in formulating codes of conduct for network data security in accordance with their charters, strengthening industry self-regulation, guiding their members to enhance network data security protection, improving the level of network data security protection, and fostering healthy industry development.

Chapter II General Rules

Article 8 No individual or organization may use network data to engage in illegal activities, nor 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 shall provide any program or tool specially designed for engaging in illegal activities referred to in the preceding paragraph. Any individual or organization clearly knowing that a person is engaging in illegal activities as mentioned in the preceding paragraph shall not provide the person with technical support such as internet access, server hosting, network storage, and communication transmission, or provide assistance in advertising promotion, payment, and the like.

Article 9 Network data processors shall, in accordance with the provisions of applicable laws, administrative regulations, and the mandatory requirements of national standards, and on the basis of the cybersecurity multi-level protection scheme, strengthen network data security protection, establish and improve network data security management system, adopt technical measures such as encryption, backup, access control, security authentication and other necessary measures to protect network data from alternation, destruction, leakage, or illegal acquisition or utilization, handle network data security incidents, prevent illegal and criminal activities targeting and exploiting network data, and bear primary responsibility for the security of network data they process.

Article 10 Network products and services provided by network data processors shall comply with the mandatory requirements of relevant national standards. When network products and services are found to have security defects, vulnerabilities, or other risks, network data processors shall take remedial measures immediately, notify users in a timely manner, and report to competent authorities concerned in accordance with regulations. Where harm to national security and public interests is involved, the network data processor shall also be required to report to the competent authorities concerned within 24 hours.

Article 11 Network data processors shall establish and improve emergency response plans for network data security incidents, and when a network data security incident occurs, shall immediately activate the plans, take measures to prevent the expansion of the harm, eliminate security risks, and report to the competent authorities in accordance with regulations.

Where any network data security incident causes harm to the legitimate rights and interests of any individual or organization, the network data processor shall notify interested parties of the security incident, as well as its risks, harmful consequences, and remedial measures already taken by such means as telephone calls, text messages, instant messaging tools, e-mail, or public announcements in a timely manner. If laws or administrative regulations prescribe that notification is not required, such provisions shall prevail. If a network data processor discovers any clue of suspected illegal or criminal activities in the process of handling a network data security incident, it shall report the case to the public security organ or the state security organ in accordance with applicable provisions, and cooperate in conducting detection, investigation, and handling work.

Article 12 Where a network data processor provides or entrusts the processing of personal information and important data to other network data processors, it shall agree on the processing purposes, means, scopes, and security protection obligations, among others, with network data recipients by contracts or other methods, and the network data processor shall supervise the performance of obligations by network data recipients. Records of the processing of personal information and important data provided or entrusted to other network data processors shall be kept for at least three years.

Network data recipients shall fulfill their obligations of network data security protection and process personal information and important data according to the agreed purposes, means, and scopes, among others.

Where two or more network data processors jointly decide on the purposes and means 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 regulations issued by the State.

Article 14 Where a network data processor needs to transfer network data due to merger, division, dissolution, bankruptcy, or any other reason, the network data recipient shall continue to fulfill its network data security protection obligations.

Article 15 Where a state organ entrusts others to construct, operate, and/or maintain e-government systems, or to store or process government data, the state organ shall undergo strict approval procedures in accordance with relevant regulations issued by the State, specify the entrusted party's network data processing authority and protection responsibilities, among others, and supervise the entrusted party's fulfillment of network data security protection obligations.

Article 16 Network data processors providing services to state organs or critical information infrastructure operators, or participating in the construction, operation, and/or maintenance of other public infrastructure or public service systems, shall fulfill their network data security protection obligations in accordance with the provisions of laws, regulations, and contracts, and provide secure, stable, and continuous services.

The network data processors specified in the preceding paragraph shall not access, obtain, retain, use, disclose, or provide others with network data, nor conduct correlation analysis of network data, without the consent of the entrusting party.

Article 17 Information systems providing services to state organs shall strengthen network data security management to ensure network data security with reference to the management requirements of e-government systems.

Article 18 Network data processors using automated tools to access and collect network data shall assess the impact on network services and must not illegally intrude into others' networks, and must not disrupt the normal operation of network services.

Article 19 Network data processors providing generative artificial intelligence services shall strengthen the security management 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 providing products or services to the public shall accept public supervision, establish convenient channels for complaints and reports on network data security, publicize information such as the methods for filing complaints and reports, and accept and handle network data security complaints and reports in a timely manner.

Chapter III Personal Information Protection

Article 21 Where network data processors, before processing personal information, inform an individual in accordance with the law by developing rules for processing personal information, such rules for processing personal information shall be centrally and publicly displayed, easily accessible, and placed in a conspicuous position. The content shall be explicit, specific, clear, and easy to understand, including but not limited to the following:

- (1) the name and contact information of the network data processor;
- (2) the purposes, means, and categories of personal information processing, the necessity of processing sensitive personal information, and the impact on individual rights and interests;
- (3) the periods of storing personal information and the method for handling such information upon expiration; and where it is difficult to determine the storage periods, the method for determining the storage periods shall be specified; and
- (4) the methods and means, among others, for individuals to access, copy, transfer, rectify, supplement, erase, and restrict the processing of their personal information, and to terminate their accounts and withdraw their consents.

Where a network data processor is required under the preceding paragraph to inform the individual of the purposes, means, and categories

of personal information to be collected and provided to other network data processors, as well as information about the recipients, such information shall be set out in the form of a list or the like. When processing personal information of minors under the age of 14, the processor shall additionally formulate specific processing rules for the handling of personal information.

Article 22 Network data processors processing personal information based on an individual's consent shall comply with the following provisions:

(1) the collection of personal information shall be necessary for providing products or services; personal information shall not be collected beyond the scope, and consent shall not be obtained through misleading, fraud, coercion, or other means;

(2) the individual's separate consent shall be obtained for processing sensitive personal information such as biometrics, religious belief, specific identity, medical health, financial accounts, and whereabouts;

(3) consent of the minor's parents or other guardians shall be obtained for processing personal information of a minor under the age of 14;

(4) personal information shall not be processed beyond the purpose, means, categories, and storage periods agreed upon by the individual;

(5) consent shall not be frequently requested after the individual has explicitly refused processing of his/her personal information; and

(6) renewed consent shall be obtained from the individual if there is any change of the purposes, means, or categories of personal information processing.

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

Article 23 Where an individual requests to access, copy, rectify, supplement, erase, or restrict the processing of his or her personal information, or deactivates an account or withdraws consent, the network data processor shall accept the requests, provide convenient methods and channels to support the exercise of these rights in a timely manner, and

shall not set unreasonable conditions to restrict reasonable requests from the individual.

Article 24 Where non-essential personal information or personal information for which consent was not obtained in accordance with the law is unavoidably collected due to the use of automated collection technology, or where an individual deactivates an account, the network data processor shall erase or anonymize such personal information. Where the storage periods stipulated by laws or administrative regulations have not expired, or it is technically difficult to erase or anonymize the personal information, the network data processor shall cease all processing other than storing and taking necessary security protection measures of such information.

Article 25 For requests for transferring personal information that meets the following conditions, a network data processor shall provide means for other network data processors designated by the individual to access and obtain relevant personal information:

- (1) the true identity of the requester can be verified;
- (2) the requested transfer involves personal information provided with the individual's consent or collected based on a contract;
- (3) the transfer of personal information is technically feasible; and
- (4) the transfer of personal information does not harm the legitimate rights and interests of others.

Where the number of transfer requests significantly exceeds a reasonable limit, the network data processor may charge necessary fees based on the cost of transferring personal information.

Article 26 Where a network data processor outside the territory of the People's Republic of China processes the personal information of any natural person in the territory, who establishes a dedicated entity or designates a representative in the territory in accordance with the provisions of Article 53 of the Personal Information Protection Law of the People's Republic of China, the network data processor shall report the name of the entity or the name and contact information of the representative to the local municipal cyberspace administration at the level of a city with districts, and the cyberspace administration shall

promptly notify the relevant competent authorities at the same level.

Article 27 Network data processors shall regularly conduct compliance audits, either on their own or by commissioning a professional agency, on their compliance with laws and administrative regulations in processing personal information.

Article 28 Network data processors processing personal information of more than 10 million individuals shall also comply with the provisions applicable to network data processors processing important data (hereinafter referred to as “important data processors”) as specified in Articles 30 and 32 of these Regulations.

Chapter IV Security of Important Data

Article 29 The coordination mechanism for national data security shall coordinate relevant competent authorities to formulate a catalog of important data and strengthen the protection of important data. All localities and departments shall, in accordance with the categorized and classified data protection system, determine specific catalogs of important data for their respective regions, departments, and relevant industries and sectors, and give priority to the network data listed in the catalogs in terms of data protection.

Network data processors shall identify and declare important data in accordance with relevant regulations issued by the State. For data confirmed as important data, the relevant region or department shall promptly inform the network data processor or make a public announcement. Network data processors shall fulfill their responsibilities for network data security protection.

The State encourages network data processors to use data tagging and other technologies and products to improve the level of important data security management.

Article 30 Important data processors shall designate a person responsible for network data security and establish a data security management body. The network data security management body shall perform the following responsibilities for network data security

protection:

(1) formulate and implement network data security management systems, operating procedures, and emergency response plans for network data security incidents;

(2) regularly organize and carry out such activities as network data security risk monitoring, risk assessment, emergency drills, publicity, education, and training, and timely respond to network data security risks and incidents; and

(3) accepting and handle complaints and reports on network data security.

The person in charge of network data security shall have specialized knowledge in network data security and relevant management experience, and shall be a member of the management team of the network data processor, and have the right to report directly to the relevant competent authorities on the situation of network data security.

Network data processors handling specific categories or scales of important data stipulated by the relevant competent authorities shall conduct a security background review of the person in charge of network data security and personnel in key positions, and strengthen training for relevant personnel. When conducting such review, they may apply for assistance from public security organs and state security organs.

Article 31 Important data processors shall conduct a risk assessment before providing, entrusting others with the processing of, or jointly processing important data with others, except for the performance of statutory duties or legal obligations.

The risk assessment shall focus on assessing the following:

(1) whether the provision, entrusted processing, and joint processing of network data, as well as the purposes, means, and scopes, among others, of processing network data by network data recipients are legitimate, justifiable, and necessary;

(2) risks of alteration, destruction, leakage, or illegal access or use of network data provided, entrusted, or jointly processed, as well as risks to national security, public interests, or the legitimate rights and interests of individuals or organizations;

(3) the integrity and compliance of network data recipients;

(4) whether the requirements for network data security specified in the relevant contract concluded or to be concluded with network data recipients can effectively bind the network data recipients to fulfill their obligations on network data security protection;

(5) whether the technical and management measures taken or to be taken can effectively prevent the risks that network data may be altered, destroyed, leaked, illegally obtained, or illegally used; and

(6) other assessment content specified by the relevant competent authorities.

Article 32 Where important data processors may affect the security of important data due to merger, division, dissolution, or bankruptcy, among others, the processors shall take measures to safeguard the security of network data and report their important data handling plans, the names and contact information of the recipients, and other information, to the relevant competent authorities at or above the provincial level; and if the relevant competent authorities are not specified, the data processors shall report to the data security work coordination mechanism at or above the provincial level.

Article 33 Important data processors shall conduct an annual risk assessment of their network data processing activities, and submit a risk assessment report to the relevant competent authorities at or above the provincial level, which shall notify the cyberspace administration and the public security organ at the same level in a timely manner.

The risk assessment report shall include the following:

(1) basic information on the network data processor, information on the network data security management body, and the name and contact information of the person responsible for network data security, among others;

(2) the purposes, categories, amounts, means, scopes, storage periods, and storage places, among others, of processing important data, and the situation of conducting network data processing activities, excluding the content of the network data itself;

(3) the network data security management system and its

implementation, technical measures such as encryption, backup, tagging, access control, security authentication, and other necessary measures and their effectiveness thereof;

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

(5) risk assessment of the provision, entrusted processing, and joint processing of important data;

(6) the situation of network data outbound transfers; and

(7) other information to be reported as specified by the relevant competent authorities.

The risk assessment report submitted by large online platform service providers processing important data shall, in addition to the contents specified in the preceding paragraph, fully specify the security of network data of key businesses and supply chains, and other circumstances.

Where important data processors engage in important data processing activities that may endanger national security, the relevant competent authorities at or above the provincial level shall order them to take measures such as rectification or cessation of processing important data. The important data processors shall immediately take measures according to relevant requirements.

Chapter V Cross-Border Security Management of Network Data

Article 34 The Cyberspace Administration of China (CAC) shall coordinate relevant competent authorities in establishing a special work mechanism for the security management of national data outbound transfer, research and formulate relevant national policies on the security management of national network data outbound transfer, and coordinate the handling of major security issues relating to network data outbound transfer.

Article 35 Network data processors may provide personal information overseas if one of the following conditions is met:

(1) they have passed the data outbound transfer security assessment

organized by CAC;

(2) they have obtained personal information protection certification from a relevant specialized institution according to the provisions issued by CAC;

(3) they comply with the provisions on standard contracts for personal information outbound transfers formulated by CAC;

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

(5) it is indeed necessary to provide the personal information of employees overseas for conducting cross-border human resource management in accordance with lawfully formulated labor rules and regulations and lawfully concluded collective contracts;

(6) it is indeed necessary to provide personal information overseas for fulfilling statutory duties or legal obligations;

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

(8) other conditions stipulated by laws, administrative regulations, or CAC.

Article 36 Where an international treaty or agreement that the People's Republic of China has concluded or acceded to stipulates conditions for providing personal information to a party outside the territory of the People's Republic of China, such stipulations may be followed.

Article 37 Where it is indeed necessary to provide an overseas party with important data collected and generated by a network data processor during its operation within the territory of the People's Republic of China, it shall pass the data outbound transfer security assessment organized by CAC. If network data processors identify and declare important data according to the relevant provisions issued by the State, which has not been informed or publicly announced by the relevant regions or departments as important data, it is not required to declare such data as important data for the data outbound transfer security assessment.

Article 38 After passing the data outbound transfer security assessment, network data processors shall not provide personal information and important data to an overseas party beyond the purposes, means, scopes, categories, or scales, among others, of the data outbound transfer specified during the assessment.

Article 39 The State takes measures to prevent and address the security risks and threats related to cross-border network data. Any individual or organization shall not provide programs or tools, among others, specially designed to destroy or circumvent technical measures, and shall not provide a person with technical support or assistance if he/she or it clearly knows that such a person engages in activities such as destroying or circumventing technical measures.

Chapter VI Obligations of Online Platform Service Providers

Article 40 Online platform service providers shall specify the network data security protection obligations of third-party product and service providers accessing their platforms through platform rules, contracts, or other methods, and urge third-party product and service providers to strengthen their network data security management.

The provisions of the preceding paragraph shall apply to the producers of smart terminals and other devices with pre-installed applications.

If third-party product or service providers violate the provisions of laws, administrative regulations, platform rules, or contractual agreements in carrying out network data processing activities, causing damage to users, the online platform service provider, the third-party product or service provider, and the producer of smart terminals and other devices with pre-installed applications, shall bear corresponding liability in accordance with the law.

The State encourages insurance companies to develop liability insurance products for network data damage compensation, and encourages online platform service providers and producers of smart terminals and other devices with pre-installed applications to purchase

such insurance.

Article 41 Online platform service providers providing application distribution services shall establish application verification rules and conduct relevant verification of network data security. If it is found that an application to be distributed or already distributed fails to comply with the provisions of laws, administrative regulations, or the compulsory requirements of national standards, measures such as warning, no distribution, and suspension or termination of distribution shall be taken.

Article 42 Online platform service providers pushing information to individuals through automated decision-making shall set up an option to turn off personalized recommendations that is easy to understand, access, and operate, and provide users with such functions as refusing to receive pushed information and erasing user tags based on their personal characteristics.

Article 43 The State promotes the development of public services for online identity authentication and popularizes and applies such services under the principles of government guidance and user voluntariness.

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

Article 44 Large online platform service providers shall publish annual social responsibility reports on personal information protection, and the contents of such reports shall include, but not be limited to, the measures for personal information protection and the effects thereof, the acceptance of applications from individuals exercising their rights, and the performance of duties by the personal information protection supervision bodies composed primarily of external members.

Article 45 Large online platform service providers engaging in the provision of network data across borders shall comply with the requirements of the State for national data cross-border security management, and improve relevant technical and administrative measures to prevent cross-border network data security risks.

Article 46 Large online platform service providers shall not use

network data, algorithms, and platform rules, among others, to engage in the following activities:

- (1) processing network data generated by users on the platform by misleading, fraud, coercion, and the like;
- (2) restricting users' access to and use of the network data generated on the platform without justifiable reasons;
- (3) implementing unreasonable differential treatment against users, which damages the legitimate rights and interests of users; and
- (4) other activities prohibited by laws or administrative regulations.

Chapter VII Supervision and Administration

Article 47 CAC is responsible for the overall planning and coordination of network data security and relevant supervision and administration.

Public security organs and national security organs shall, in accordance with the provisions of relevant laws, administrative regulations, and these Regulations, undertake the responsibilities for supervising and administering network data security within the scope of their respective duties, and legally prevent and crack down on illegal and criminal activities that endanger network data security.

The National Data Administration shall perform corresponding duties for network data security when undertaking specific data management work.

All localities and departments shall bear responsibility for the network data collected and generated in their work within their region or department and for its security.

Article 48 Relevant competent authorities shall assume the responsibilities of supervising and administering network data security within their respective industries and sectors. They shall specify the work bodies responsible for network data security protection in their respective industries and sectors, coordinate the formulation and organize the implementation of emergency response plans for network data security incidents in their respective industries and sectors, regularly organize the assessment of network data security risks in their respective industries

and sectors, supervise and inspect network data processors' fulfillment of network data security protection obligations, and direct and urge network data processors to rectify existing and potential risks in a timely manner.

Article 49 CAC shall coordinate relevant competent authorities in collecting, assessing, sharing, and publishing information relating to network data security risks in a timely manner, and strengthen network data security information sharing, monitoring and early warning of network data security risks and threats, and emergency response to network data security incidents.

Article 50 Relevant competent authorities may take the following measures to supervise and inspect network data security:

(1) requiring a network data processor and its relevant personnel to provide explanations regarding the matters under supervision and inspection;

(2) retrieving and duplicating the documents and records relating to network data security;

(3) checking the implementation of network data security measures;

(4) checking the equipment and items relating to network data processing activities; and

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

Network data processors shall cooperate with the network data security supervision and inspection conducted by the relevant competent authorities in accordance with the law.

Article 51 Relevant competent authorities shall conduct supervision and inspection of network data security in an objective and impartial manner, and shall not charge fees from the inspected entities.

During the supervision and inspection of network data security, the relevant competent authorities shall not access or collect business information irrelevant to network data security, and the information obtained may only be used for the purpose of maintaining network data security and shall not be used for any other purpose.

Where discovering that there are relatively high security risks in the network data processing activities conducted by a network data processor,

the relevant competent authorities may, according to prescribed authority and procedures, require the network data processor to suspend relevant services, modify platform rules, improve technical measures, or take other actions, to eliminate potential network data security risks.

Article 52 When carrying out supervision and inspection of network data security, relevant competent authorities shall strengthen coordination, cooperation, and information communication, and reasonably determine the frequency and methods of inspection, so as to avoid unnecessary and overlapping inspections.

The compliance audit in respect of personal information protection, risk assessment of important data, and security assessment for important data outbound transfer, among others, shall be connected more closely to avoid repeated assessments and audits. If any content in the risk assessment of important data overlaps with that in the cybersecurity multi-level protection assessment, the relevant results can be mutually recognized.

Article 53 Relevant competent authorities and their staff members shall legally keep confidential the network data such as personal privacy, personal information, trade secrets, and confidential business information to which they have access in the performance of their duties, and shall not disclose such data or illegally provide such data to others.

Article 54 Where overseas organizations or individuals engage in network data processing activities that endanger the national security or public interests 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, CAC may, in conjunction with relevant competent authorities, take corresponding necessary measures in accordance with the law.

Chapter VIII Legal Liability

Article 55 Where anyone violates the provisions of Article 12, Articles 16 to 20, Article 22, paragraphs 1 and 2 of Article 40, Article 41, or Article 42 of these Regulations, cyberspace administration,

telecommunications administration, and public security organ, among others, shall, according to their respective duties, order the violator to make corrections, give a warning, and confiscate the illegal gains of the violator; where the violator refuses to make corrections or the circumstances are serious, relevant competent authorities shall impose a fine of not more than RMB 1,000,000 Yuan on the violator, may order the suspension of relevant business, or order the suspension of all the business operations for rectification, revoke relevant business permit or license, and shall impose a fine of not less than RMB 10,000 Yuan but not more than RMB 100,000 Yuan on the directly liable person in charge and other directly liable persons.

Article 56 Where anyone violates the provisions of Article 13 of these Regulations, cyberspace administration, telecommunications administration, public security organ, and national security organ, among others, shall, according to their respective duties, order the violator to make corrections, give a warning, and may impose a fine of not less than RMB 100,000 Yuan but not more than RMB 1,000,000 Yuan on the violator, and impose a fine of not less than RMB 10,000 Yuan but not more than RMB 100,000 Yuan on the directly responsible person in charge and other directly liable persons. If the violator refuses to take corrective action or the circumstances are serious, the relevant competent authorities shall impose a fine of not less than RMB 1,000,000 Yuan but not more than RMB 10,000,000 Yuan on the violator, may order the suspension of relevant business, or order the suspension of all the business operations for rectification, revoke relevant business permit or license, and shall impose a fine of not less than RMB 100,000 Yuan but not more than RMB 1,000,000 Yuan on the directly liable person in charge and other directly liable persons.

Article 57 Where anyone violates the provisions of paragraph 2 of Article 29, paragraphs 2 and 3 of Article 30, Article 31, or Article 32 of these Regulations, cyberspace administration, telecommunications administration, and public security organ, among others, shall, according to their respective duties, order the violator to make corrections, give a warning, and may impose a fine of not less than RMB 50,000 Yuan but

not more than RMB 500,000 Yuan on the violator, and impose a fine of not less than RMB 10,000 Yuan but not more than RMB 100,000 Yuan on the directly responsible person in charge and other directly liable persons. If the violator refuses to take corrective action or causes large-scale data leakage or other serious consequences, the relevant competent authorities shall impose a fine of not less than RMB 500,000 Yuan but not more than RMB 2,000,000 Yuan on the violator, may order the suspension of relevant business, or order the suspension of all the business operations for rectification, revoke relevant business permit or license, and shall impose a fine of not less than RMB 50,000 Yuan but not more than RMB 200,000 Yuan on the directly liable person in charge and other directly liable persons.

Article 58 Whoever, in violation of other relevant provisions of these Regulations shall be held legally liable by the relevant competent authorities in accordance with the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China, and other applicable laws.

Article 59 Network data processors who take the initiative to eliminate or mitigate the harmful consequences of their illegal act, commit any minor illegal act and take corrective action in a timely manner without causing harmful consequences, or commit any illegal act for the first time with minor harmful consequences and take corrective action in a timely manner, shall be subject to 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 fulfill the network data security protection obligations provided in these Regulations, the organs at the higher level or the relevant competent authorities shall order it to make corrections and give sanctions to the directly responsible person in charge and other directly liable persons in accordance with the law.

Article 61 Whoever, in violation of these Regulations, causes damage to others shall bear civil liability in accordance with the law.

Where a violation of public security administration is constituted, a public security administration penalty shall be given in accordance with the law. Where a crime is constituted, criminal responsibility 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” refers to various electronic data processed and generated through networks.

(2) “network data processing activities” refer to the collection, storage, use, processing, transmission, provision, disclosure, erasure, and other activities of network data.

(3) “network data processor” refers to an individual or organization that autonomously determines the purposes and means of processing in network data processing activities.

(4) “important data” refers to data in specific fields, pertaining to specific groups or regions, or reaching a certain level of accuracy and scale, which, if altered, destroyed, leaked, or illegally obtained or utilized, may directly endanger national security, economic operation, social stability, or public health and security.

(5) “entrusted processing” refers to the network data processing activities carried out by any individual or organization entrusted by a network data processor according to the agreed purposes and means.

(6) “joint processing” refers to network data processing activities in which two or more network data processors jointly determine the purposes and means of processing the network data.

(7) “separate consent” refers to specific and explicit consent given by an individual specifically for a particular processing activity of his or her personal information.

(8) “large online platform” refers to an online platform with 50 million or more registered users or 10 million or more monthly active users, with complex business types, and whose network data processing activities have a significant impact on national security, economic

operation, national economy, and the people's livelihood, among others.

Article 63 Network data processing activities involving core data shall be carried out in accordance with the relevant provisions issued by the State.

These Regulations are not applicable where a natural person processes personal information for personal or family affairs.

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

Article 64 These Regulations shall be effective as of January 1, 2025.

本译本仅供参考，若有歧义，请以中文版本为准。

The English version is for reference only. In case of any discrepancy or ambiguity of meaning between this English translation and the Chinese version, the latter shall prevail.