GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GB/T 41479-2022

Information security technology - Network data processing security requirements

信息安全技术 网络数据处理安全要求

Issued on: April 15, 2022 **Implemented on: November 01, 2022**

Issued by: State Administration for Market Regulation;
Standardization Administration of the People's Republic of China.

Table of Contents

Information security technology - Network data processing security requirements

1 Scope

This document specifies the security technology and management requirements for network operators to collect, store, use, process, transmit, provide, and disclose network data.

This document applies to the regulation of network data processing by network operators, as well as the supervision, management and evaluation of network data processing by regulatory authorities and third-party evaluation agencies.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the version corresponding to that date is applicable to this document; for undated references, the latest version (including all amendments) is applicable to this document.

GB/T 25069, Information security technology - Glossary

GB/T 35273-2020, Information security technology - Personal information security specification

3 Terms and definitions

Terms and definitions determined by GB/T 25069 and GB/T 35273-2020, as well as the following ones, are applicable to this document.

3.1

Data

Any recording of information electronically or otherwise.

3.2

Network data

All kinds of data collected, stored, used, processed, transmitted, provided and disclosed through the network.

Examples: personal information, important data, etc.

3.3

Data processing

Data collection, storage, use, processing, transmission, provision, disclosure, etc.

3.4

Data security

By taking necessary measures, ensure that the data is in a state of effective protection and legal use, and has the ability to ensure a continuous security state.

3.5

Network operator

Network owner, manager and network service provider.

Note: The network in this document refers to the open and public network.

3.6

Personal Information

Various information recorded electronically or otherwise relating to an identified or identifiable natural person.

Note 1: Personal information includes name, date of birth, citizenship number, personal biometric information, address, communication contact information, communication records and content, account password, property information, credit information, whereabouts, accommodation information, health and physiology information, transaction information, etc.

Note 2: It does not include anonymized information.

[Source: GB/T 35273-2020, 3.1, modified]

3.7

Sensitive personal information

The personal information which, once leaked or illegally used, is likely to cause damage to the personal dignity of a natural person or endanger personal and property safety.

Note: Sensitive personal information includes biometrics, religious beliefs, specific identities, medical treatment and health, financial accounts, whereabouts and

Anonymization

The process of processing personal information to a state where it does not identify a specific natural person and cannot be recovered.

4 General requirements for data processing security

4.1 Data identification

Network operators shall identify the data involved in data processing, including personal information, important data and other data, form a data protection catalog, and update it in a timely manner.

4.2 Classification and gradation

Network operators shall, in accordance with relevant national standards, according to contract provisions and business operation needs, conduct classification and gradation of the identified data.

4.3 Risk prevention and control

Network operators shall perform data security protection obligations in accordance with the contract when carrying out data processing, and strengthen risk monitoring when carrying out data processing activities. In case of data security flaws, loopholes and other risks, technologies such as encryption, desensitization, backup, access control, auditing, or other necessary measures shall be adopted to strengthen data security protection and protect data from leakage, theft, tampering, damage, and improper use. When providing key protection for important data and sensitive personal information, regular risk assessments of the data processing activities shall be carried out in accordance with regulations, and risk assessment reports shall be submitted to the relevant competent authorities. The risk assessment report shall include the type and quantity of important data processed, the situation of data processing activities, the data security risks faced and countermeasures, etc.

Data security management responsibility and evaluation and assessment systems shall be established, data security protection plans shall be formulated, security risk assessments shall be carried out, security incidents shall be dealt with in a timely manner, and education and training shall be organized.

4.4 Auditing and traceability

Network operators shall record the entire life cycle of data processing to ensure that data processing is auditable and traceable.

5 Data processing security technical requirements

5.1 General

Network operators shall conduct impact analysis and risk assessment when carrying out data processing, and take necessary measures to control the identified risks to ensure data security. In the event of a public health emergency, data processing shall also comply with the requirements of Appendix A. Data processing activities that affect or may affect national security shall be subject to national security review.

5.2 Collection

Where the network operator needs to process personal information in order to provide services, it shall follow the principles of legality, legitimacy and necessity, and shall not collect personal information that is not directly or reasonably related to the services it provides, or that exceeds the period of express consent of the personal information subject, and shall comply with the following requirements:

a) A personal information protection policy shall be formulated and disclosed and strictly followed; the personal information protection policy shall meet the requirements of 5.5 in GB/T 35273-2020;

b) Before collecting personal information, the personal information protection policy shall be clearly stated and the consent of the personal information subject shall be obtained;

Note: Except for the situations specified in 5.6 of GB/T 35273-2020.

c) Where the purpose, type, scope, and use of processed personal information are changed, the personal information subject shall be informed in time, the personal information protection policy shall be revised, and the consent of the personal information subject shall be re-obtained. Where it involves changes in the personal information protection policy, the personal information protection policy shall be revised;

d) Express the type of product or service provided and the personal information necessary for the product or service; shall not refuse to provide the product or service because the user does not agree or withdraws consent to provide information other than the personal information necessary for the product or service;

e) It shall not force or mislead users to agree to the collection of personal information only for the purpose of improving service quality, enhancing user experience, pushing information in a targeted manner, developing new products, etc.;

b) In the process of providing news and blog information services to personal information subjects, if network operators use algorithms to automatically synthesize text, pictures, audio and video and other information, and they shall clearly inform users.

5.4.2 Third party application management

Network operators shall strengthen data security management for third-party applications that access or embed their products or services, including:

a) The data security protection responsibilities and obligations of both parties shall be clearly defined through contracts and other forms;

b) Third party application operators shall be supervised to strengthen data security management; if third party applications are found to have not fulfilled the security management responsibilities, they shall promptly urge rectification and stop access when necessary;

c) If the network operator knows or shall know that the third party application uses its platform to infringe the civil rights and interests of users, and fails to take necessary measures, it shall bear joint and several liability with the third-party application operator;

d) It is advisable to carry out technical testing on the access or embedded third party applications to ensure that their data processing behaviors meet the requirements agreed upon by both parties, and stop access in a timely manner if the audit finds that the behavior exceeds the agreement between the two parties.

5.5 Processing

In the process of data processing activities such as conversion, aggregation, and analysis, network operators who know or shall know that it may endanger national security, public security, economic security and social stability shall immediately stop the processing activities.

5.6 Transmission

Network operators shall take security measures for data transmission activities, including:

a) When transmitting important data and sensitive personal information, security measures such as encryption and desensitization shall be adopted;

b) When transmitting data to the data receiver, security measures shall be taken as required and agreed upon in the contract.

5.7 Provision

5.7.1 Providing to others

Before providing data to others, network operators shall conduct security impact analysis and risk assessment. Those that may endanger national security, public security, economic security and social stability shall not be provided to others. Requirements are as follows:

a) When providing personal information to others, the personal information subject shall be informed of the receiver's name, contact information, processing purpose, processing method, type of personal information, and storage period, and the consent of the personal information subject shall be obtained;

b) When sharing or transferring important data, the data security protection responsibilities and obligations of both parties shall be clarified with the data receiver through contracts and other forms, and measures such as encryption and desensitization shall be adopted to ensure the security of important data;

c) If a third party is entrusted to carry out data processing activities, the purpose, duration, processing method, type of data, protection measures, rights and obligations of both parties, and the method of returning or deleting data by the third party shall be clearly stipulated in the form of a contract, etc. The third party is required to return and delete received and generated data in the form agreed in the contract, and the data processing activities shall be supervised;

d) In the event of acquisition, merger, reorganization or bankruptcy, the data receiver shall continue to perform relevant data security protection obligations; if there is no data receiver, the data shall be deleted.

5.7.2 Data export

When network operators provide personal information or important data overseas, they shall follow the requirements of relevant national regulations and standards.

If domestic users access domestic networks within China, their flow shall not be routed overseas.

5.8 Disclosure

Network operators shall not endanger national security, public security, economic security and social stability when using the data resources at their disposal to disclose market forecasts, statistics and other information.

b) For key operations of important data and personal information (such as batch modification, copying, deletion, downloading, etc.), set up internal approval and audit processes, and strictly implement them.

5.13 Data deletion and anonymization

When meeting the requirements of 8.3 in GB/T 35273-2020 or meeting the following circumstances, network operators shall delete or anonymize personal information in a timely manner:

a) When personal information exceeds the storage period agreed by both parties;

b) When network products and services cease to operate;

c) When the personal information subject cancels the account, or when the user withdraws consent.

When the media storing important data and personal information is scrapped, network operators shall destroy the media by physical damage to ensure that important data and personal information cannot be recovered.

6 Data processing security management requirements

6.1 Responsible person for data security

When network operators carry out business and service activities, and handle important data and sensitive personal information, they shall identify the person responsible for data security, and provide them with necessary resource guarantees to ensure that they independently perform their duties. The person in charge of data security shall have professional knowledge of data security and relevant management experience, participate in important decisions about data processing, and perform the following responsibilities:

a) Organize the determination of the data protection catalogue, formulate the data security protection plan and supervise the implementation;

b) Organize and carry out data security impact analysis and risk assessment, and supervise the rectification of potential security risks;

c) Report data security protection and incident handling to relevant departments in accordance with the law;

d) Organize to accept and handle data security complaints and reports.

6.2 Human resource assurance and assessment

In terms of human resource assurance and assessment, network operators shall:

a) Clarify data security protection positions and responsibilities, and provide human resource guarantees.

b) Establish a human resources assessment system, clarify data security management assessment indicators and accountability mechanisms, and assess the performance of relevant personnel, especially those in important positions. In the event of a major incident of data security, the directly responsible supervisor and other directly responsible personnel shall be held accountable.

6.3 Incident emergency response

Network operators shall establish an emergency response mechanism for data security incidents, and make timely adjustments according to changes in data security plans to ensure that data security incidents are dealt with in a timely and effective manner.

a) Emergency response mechanisms include:

1) Data security incident gradation;

2) Start-up condition;

3) Resources required for start-up, such as personnel, equipment, premises, tools, funds, etc.;

4) Procedures, personnel arrangements and operation manuals.

b) Equip with the resources required for emergency response to ensure that the emergency response mechanism can be effectively implemented.

c) Formulate an emergency drill plan, organize emergency drills according to the plan or after the emergency response mechanism changes, test and improve the emergency response mechanism, and improve the actual combat capability.

In the event of a data security incident, the network operator shall immediately activate the emergency response mechanism and take corresponding remedial and preventive measures. Where personal information is involved, the personal information subject shall be notified by telephone, text message, email or letter in a timely manner; at the same time, those that may endanger national security, public security, economic security and social stability shall be reported to relevant departments according to relevant requirements.

In order to control the expansion of the incident and reduce the harm of the incident, where the designated agency really needs to use the personal information that has been collected, it shall adhere to the principle of minimization, and strictly limit the scope, scale, quantity and the lookback time span of whereabouts information of the personal information used according to the actual needs of responding to public health emergencies. It shall be approved by the relevant command department, or by the health administrative department of the State Council in conjunction with the relevant industry management department, and the scope, type and procedure of personal information called shall be clarified, and the personal information subject shall be informed.

A.5 Face recognition verification

In the process of providing information services, designated institutions should provide other authentication methods for users to choose when face recognition is used as the authentication method.

Where face recognition information is used for identity verification, the original image from which face recognition information can be extracted should not be kept.

A.6 Information access service

Designated institutions that provide information access services shall be able to verify the identity of the access person through domestic mobile phone numbers and other means that can confirm the identity, to prevent unauthorized access to other people's personal information.

A.7 Disclosing, providing personal information to others and changing the use of personal information

Personal information collected and mastered by designated institutions shall not be disclosed or illegally provided to others without the consent of the personal information subject, and shall not be changed for use. If it is really necessary to disclose, provide to others or change the use, the consent of the personal information subject shall be obtained. If it is urgent or the consent is inconvenient to obtain, it shall be reported to the emergency command department or the health administrative department of the State Council for consent, and the personal information subject shall be informed in a timely manner.

Designated institutions shall not use the personal information they have mastered or the convenience of providing information services to seek commercial interests, including marketing, targeted advertising, etc.

A.8 Handling personal information after work

After the public health emergency response work is completed, the designated agency shall stop collecting and calling personal information, and delete the personal information that has been collected and called during the public health emergency

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------