GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 35273-2020

Replacing GB/T 35273-2017

Information security technology - Personal information security specification

信息安全技术 个人信息安全规范

Issued on: March 06, 2020 **Implemented on: October 01, 2020**

Issued by: State Administration for Market Regulation;

Standardization Administration of PRC.

Table of Contents

Information security technology - Personal information security specification

1 Scope

This standard specifies the principles and security requirements for carrying out personal information processing activities such as collection, storage, use, sharing, transfer, public disclosure, deletion, etc.

This standard is applicable to regulate personal information processing activities of various organizations, as well as the supervision, management and evaluation of personal information processing activities by organizations such as competent regulatory authorities and third-party evaluation agencies.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB/T 25069-2010 Information security technology - Glossary

3 Terms and definitions

The terms and definitions as defined in GB/T 25069-2010 as well as the following terms and definitions apply to this document.

3.1

Personal information

Various information recorded electronically or in other ways that can identify the identity of a particular natural person or reflect the activities of a particular natural person, alone or in combination with other information.

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

The act of gaining control of personal information.

Note 1: This includes activities such as being actively provided by personal information subjects, automatic collection activities such as interacting with personal information subjects or recording the activities of personal information subjects, as well as indirectly acquiring personal information through sharing, transfer, and collection of public information.

Note 2: If the provider of the product or service provides tools for the use of personal information subjects, whilst the provider does not access personal information, it does not belong to the collection referred to in this standard. For example, after the offline navigation software obtains the personal information subject's position information from the terminal, if it does not transfer it back to the software provider, it does not belong to the collection of personal information subject's position information.

3.6

Explicit consent

The personal information subject actively makes statements in paper or electronic form in written, oral, etc., or autonomously makes affirmative actions, to make explicit authorization for the specific processing of their personal information.

Note: Affirmative actions include active selection of personal information subjects, active clicks on "agree", "register", "send" and "dial", active filling or providing, etc.

3.7

Consent

Subjects of personal information make specific authorizations for specific processing of their personal information.

Note: Including authorization through active actions (i.e., explicit consent), or authorization through negative omissions (e.g., personal information subjects in the information collection area did not leave the area after being informed of the information collection behavior).

3.8

User profiling

The process of collecting, aggregating and analyzing personal information, analyzing or predicting individual characteristics of a specific natural person, such as occupation, economy, health, education, personal preferences, credit, behavior, etc., to form its personal characteristic model.

The process of processing personal information so that the personal information subject cannot be identified or associated, meanwhile the processed information cannot be recovered.

Note: The information obtained after anonymizing personal information is not personal information.

3.15

De-identification

The process of technical processing of personal information, to make it is impossible to identify or associate the personal information subject without resorting to additional information.

Note: De-identification is based on the individual, retains the individual granularity, uses pseudonyms, encryption, hash functions and other technical means to replace the identification of personal information.

3.16

Personalized display

Based on personal information such as the web browsing history, interests and hobbies, consumption records and habits of a specific personal information subject, the activities of displaying information content and providing search results for goods or services, etc. to the personal information subject.

3.17

Business function

The type of service that meets the specific use needs of personal information subjects.

Note: Such as map navigation, online car booking, instant messaging, online community, online payment, news information, online shopping, express delivery, transportation ticketing, etc.

4 Basic principles of personal information security

Personal information controllers shall follow the legal, legitimate and necessary principles for carrying out personal information processing activities, including:

a) Consistent rights and responsibilities - Take technical and other necessary measures to ensure the security of personal information; take

a) The type of personal information collected shall be directly related to the realization of the business function of the product or service; direct association means that without the participation of the above personal information, the function of the product or service cannot be realized.

b) The frequency of automatically collecting personal information shall be the minimum frequency necessary to realize the business function of the product or service.

c) The amount of indirect access to personal information shall be the minimum amount necessary to realize the business function of the product or service.

5.3 Independent choice of multiple business functions

When a product or service provides multiple business functions that require the collection of personal information, the personal information controller shall not violate the autonomous will of the personal information subject and force the personal information subject to accept the business function provided by the product or service and the corresponding personal information collection request. Requirements for personal information controllers include:

a) The personal information subject shall not be required to accept and authorize the request for the collection of personal information for business functions that have not been applied for or used at one time by bundling various business functions of products or services.

b) Affirmative actions independently made by the personal information subject, such as active click, check and fill-in shall be used as the enabling conditions for specific business functions of products or services. The personal information controller shall start collecting personal information only after the personal information subject starts the business function.

c) The way or method of closing or withdrawing the business function shall be as convenient as the way or method the personal information subject chooses to use the business function. After the personal information subject chooses to close or withdraw from a specific business function, the personal information controller shall stop the collection of personal information for that business function.

d) If the personal information subject does not authorize the consent to use, shut down or withdraw from a specific business function, the authorized consent of the personal information subject shall not be frequently sought.

e) If the personal information subject does not authorize the consent to use, shut down or withdraw from a specific business function, it shall not

Note 3: When the personal information subject first turns on a product or service, registers an account, etc., it should actively display the main or core content of the personal information protection policy to him in the form of a pop-up window, etc. to help the personal information subject understand the scope and rules for processing personal information of this product or service, thereby deciding whether to continue to use the product or service.

5.6 Exceptions with authorized consent

In the following situations, the personal information controller does not need to obtain the consent of the personal information subject to collect and use personal information:

a) Relevant to the personal information controller's performance of its obligations under laws and regulations;

b) Directly related to national security and national defense security;

c) Directly related to public security, public health, major public interests;

d) Directly related to criminal investigation, prosecution, trial and judgment execution;

e) Out of the protection of the important legal rights and interests of the personal information subject or other individuals' lives, property, etc., but it is difficult to obtain consent;

f) The personal information involved is disclosed to the public by the personal information subject;

g) Necessary to sign and perform the contract according to the requirements of the personal information subject;

Note: The main function of the personal information protection policy is to disclose the scope and rules for the collection and use of personal information by the personal information controller; it should not be regarded as a contract.

h) Collect personal information from legally publicly disclosed information, such as legal news reports, government information disclosure and other channels;

i) Necessary to maintain the secure and stable operation of the products or services provided, such as discovering and handling failures of products or services;

j) The personal information controller is a news organization, meanwhile it is necessary to carry out legal news reports;

1) Only store summary information of personal biometric information;

2) Use personal biometric information directly in the collection terminal to achieve functions such as identity recognition and authentication;

3) When using facial recognition features, fingerprints, palm prints, irises, etc. to realize identity recognition, authentication and other functions, delete the original image wherein the personal biometric information can be extracted.

Note 2: The summary information is usually irreversible and cannot be traced back to the original information.

Note 3: Except for the situation where the personal information controllers fulfill their obligations under laws and regulations.

6.4 Personal information controller ceases operations

When the personal information controller stops operating its products or services, it shall:

a) Stop collecting personal information in time;

b) Notify the personal information subject in the form of one-by-one delivery or announcement;

c) Delete or anonymize the personal information it holds.

7 Use of personal information

7.1 Access control measures for personal information

Requirements for personal information controllers include:

a) For those authorized to access personal information, a minimum authorized access control strategy shall be established, so that they can only access the minimum necessary personal information required for their duties, meanwhile only have the minimum data operation authority required to complete their duties;

b) Set up internal approval processes for important operations of personal information, such as batch modification, copying, downloading and other important operations;

c) Separately set the roles of security management personnel, data

information can identify the identity of a specific natural person or reflect the activities of a specific natural person, alone or in combination with other information, it shall be considered as personal information. It shall be handled within the scope of the consent obtained when collecting personal information.

Note 2: If the personal information generated by processing is personal sensitive information, its processing must meet the requirements for personal sensitive information.

7.4 Restrictions on the use of user profiling

Requirements for personal information controllers include:

a) The description of the characteristics of the personal information subject in the user profiling shall not:

1) Contains obscenity, pornography, gambling, superstition, terror, violence;

2) Express content that discriminates against ethnicity, race, religion, disability, disease.

b) Those who use user profiling in business operations or foreign business cooperation shall not:

1) Infringe upon the lawful rights and interests of citizens, legal persons and other organizations;

2) Endanger national security, honor and interests; incite overturning state power, overthrowing the socialist system; incite to split the country; undermine national unity; promote terrorism, extremism, national hatred, ethnic discrimination; spread violent and obscene pornographic information; make up and disseminate false information to disturb economic and social order.

c) In addition to being necessary for the purpose of authorized use of the personal information subject, the use of personal information shall eliminate clear identity orientation and avoid precise positioning to specific individuals. For example, in order to accurately evaluate personal credit status, direct user profiling can be used; for the purpose of pushing commercial advertisements, it should use indirect user profiling.

7.6 Convergence and fusion of personal information collected for different business purposes

Requirements for personal information controllers include:

a) It shall comply with the requirements of 7.3;

b) It shall, according to the purpose for which personal information is aggregated and infused, carry out an impact assessment of personal information security; take effective personal information protection measures.

7.7 Use of information system's automatic decision-making mechanism

The information system used by the personal information controller's business operations shall, when it has an automatic decision-making mechanism and can significantly affect the rights of personal information subjects (for example, automatic determination of personal credit and loan quotas, or automated screening for interviewers, etc.):

a) Carry out personal information's security impact assessment at the planning and design stage or before the first use; take effective measures to protect the personal information subject according to the assessment results;

b) Regularly (at least once a year) conduct a personal information's security impact assessment during the use process; improve the measures for protecting the personal information subject based on the assessment results;

c) Provide personal information subjects with complaint channels for automatic decision-making results and support manual review of automatic decision-making results.

8 Rights of personal information subjects

8.1 Inquiry of personal information

The personal information controller shall provide the personal information subject with a method to query the following information:

8.6 in a timely manner. It shall, within 30 days or within the time limit prescribed by laws and regulations, make a response and reasonable explanation; meanwhile notify the personal information subject of the resolution of external disputes.

b) If interactive pages (such as websites, mobile Internet applications, client software, etc.) are used to provide products or services, it should directly set up convenient interactive pages to provide functions or options, so that personal information subjects can exercise their rights of access, correction, deletion, withdrawal of consent, cancellation of accounts, etc.

c) In principle, no fee is charged for reasonable requests; however, for repeated requests within a certain period of time, a certain cost may be charged as appropriate.

d) If directly fulfilling the request of the personal information subject requires high costs or causes other significant difficulties, the personal information controller shall provide an alternative method to the personal information subject, to protect the legitimate rights and interests of the personal information subject.

e) In the following cases, it may not respond to requests from personal information subjects based on 8.1 ~ 8.6, including:

1) Related to the personal information controller's fulfillment of obligations under laws and regulations;

2) Directly related to national security and national defense security;

3) Directly related to public security, public health, major public interests;

4) Directly related to criminal investigation, prosecution, trial and execution of judgments;

5) The personal information controller has sufficient evidence that the personal information subject is subjectively malicious or abuses his rights;

6) Out of the protection of the significant legal rights and interests of the personal information subject or other individuals' lives, property, etc., but it is difficult to obtain his consent;

7) Responding to the request of the personal information subject will result in serious damage to the legal rights of the personal information subject or other individuals and organizations;

8) Involving trade secrets.

personal information, it shall promptly feed back to the personal information controller.

5) No more personal information will be stored when the entrusting relationship is released.

d) The personal information controller shall supervise the entrusted party, in a way including but not limited to:

1) Specifying the responsibilities and obligations of the entrusted party through contracts and other means;

2) Auditing the entrusted party.

e) The personal information controller shall accurately record and store the entrusted processing of personal information.

f) If the personal information controller learns or finds that the entrusted party does not process the personal information in accordance with the entrusted requirements, or fails to effectively fulfill the security protection responsibility for personal information, it shall immediately request the entrusted party to stop the relevant actions; take or request the entrusted party to take effective remedy measures (such as changing passwords, recovering permissions, disconnecting network connections, etc.) to control or eliminate the security risks faced by personal information. When necessary, the personal information controller shall terminate the business relationship with the entrusted party, meanwhile request the entrusted party to delete the personal information obtained from the personal information controller in a timely manner.

9.2 Sharing and transfer of personal information

When personal information controllers share and transfer personal information, they shall pay full attention to risks. The sharing and transfer of personal information, not due to acquisition, merger, reorganization, or bankruptcy, shall meet the following requirements:

a) Conduct a personal information's security impact assessment in advance; take effective measures to protect the personal information subject based on the assessment results.

b) Inform the personal information subject about the purpose of sharing and transferring personal information, the type of data receiver and possible consequences; obtain the prior authorization of the personal information subject. Except for sharing and transferring personal information that has been de-identified, meanwhile ensuring that the data receiver cannot re-

9.3 Transfer of personal information during acquisition, merger, reorganization, bankruptcy

When the personal information controller is subject to changes such as acquisition, merger, reorganization, bankruptcy, etc., the requirements for the personal information controller include:

a) Inform relevant information to the personal information subject;

b) The changed personal information controller shall continue to fulfill the responsibilities and obligations of the original personal information controller. If the purpose of using personal information is changed, it shall obtain the explicit consent of the personal information subject again;

c) If bankruptcy and no undertaking, delete the data.

9.4 Public disclosure of personal information

In principle, personal information shall not be publicly disclosed. When the personal information controller is authorized by law or has reasonable grounds for public disclosure, it shall meet the following requirements:

a) Conduct a personal information's security impact assessment in advance; take effective measures to protect the personal information subject based on the assessment results;

b) Inform the personal information subject of the purpose and type of public disclosure of personal information; obtain the explicit consent of the personal information subject in advance;

c) Before publicly disclosing personal sensitive information, in addition to the content notified in b), the personal information subject shall be informed of the content of personal sensitive information involved;

d) Accurately record and store the public disclosure of personal information, including the date, scale, purpose, scope of public disclosure;

e) Bear the corresponding responsibility for the damage to the legitimate rights and interests of the personal information subject as caused by the public disclosure of personal information;

f) Personal biometric information shall not be publicly disclosed;

g) The analysis results of personal sensitive data such as race, ethnicity, political views, religious beliefs of our citizens shall not be publicly

information controller shall bear the responsibility for personal information security caused by the third party.

Note: If the personal information controller deploys a third-party plug-in that collects personal information in the process of providing products or services (for example, website operators and deployed statistical analysis tools in applications, software development kit SDKs, call map API interface), meanwhile the third party does not separately obtain the consent of the personal information subject to collect personal information, then the personal information controller and the third party are joint personal information controllers at the stage of personal information collection.

9.7 Third-party access management

When a personal information controller accesses a third-party product or service with the function of collecting personal information in its products or services and 9.1 and 9.6 are not applicable, the requirements for the personal information controller include:

a) Establish a third-party product or service access management mechanism and workflow; if necessary, establish a security assessment mechanism to set access conditions;

b) The security responsibilities of both parties and the personal information security measures to be implemented shall be clarified with third-party product or service providers through contracts and other forms;

c) The personal information subject shall be clearly identified that the product or service is provided by a third party;

d) It shall properly retain the relevant contracts and management records on the third party's access to the platform, to ensure that they can be accessed by relevant parties;

e) Third parties shall be required to obtain consent for the collection of personal information from the personal information subject in accordance with the relevant requirements of this standard; it shall verify the way of its realization if necessary;

f) Third-party products or services shall be required to establish a mechanism to respond to requests and complaints from personal information subjects, so that the personal information subjects can carry out query and use;

g) Third-party products or service providers shall be supervised to strengthen the security management of personal information. If it finds that the third-party products or services have not implemented the security management requirements and responsibilities, they shall promptly rectify

3) Formulate, issue, implement, regularly update personal information protection policies and related procedures;

4) Establish, maintain and update the list of personal information held by the organization (including the type, quantity, source, recipient, etc. of personal information) and authorized access strategy;

5) Carry out personal information's security impact assessment; put forward countermeasures and suggestions for personal information protection; urge the rectification of hidden security risks;

6) Organize personal information security training;

7) Perform testing before the product or service is launched, to avoid unknown personal information collection, use, sharing and other processing behaviors;

8) Publish information such as complaints and reporting methods and receive complaint reports in a timely manner;

9) Conduct security audit;

10) Maintain communication with supervisory and administrative departments; notify or report the personal information protection and incident handling, etc.

e) The person in charge of personal information protection and the organization of personal information protection shall be provided with the necessary resources to ensure their independent fulfillment of duties.

11.2 Personal information security engineering

When developing products or services with the function of processing personal information, personal information controllers should consider personal information protection requirements at the stage of system engineering such as demand, design, development, testing, release in accordance with relevant national standards, to ensure the protection measures of personal information during system construction are simultaneously planned, constructed, put into use.

11.3 Records for personal information processing activity

The personal information controller should establish, maintain and update the records for the processing activity of collected and used personal information, which may include:

Appendix B

(Informative)

Determination of personal sensitive information

Personal sensitive information refers to personal information that, once disclosed, illegally provided or misused, may endanger the security of persons and property, easily lead to damage to personal reputation, physical and mental health, or discriminatory treatment. Usually, personal information of children under 14 years old (inclusive) and information related to the privacy of natural persons are personal sensitive information. It can determine whether it is personal sensitive information from the following angles:

Disclosure: Once the personal information is disclosed, it will cause the personal information subject and the organizations and institutions that collect and use personal information to lose the ability to control the personal information, resulting in the uncontrollable scope and use of personal information. After the disclosure of certain personal information, it is directly used in a manner contrary to the will of the personal information subject or associated analysis with other information, which may bring significant risks to the personal information subject's rights and interests, then it shall be determined as personal sensitive information. For example, the copy of the identity card of the personal information subject is used by others for real-name registration of mobile phone number cards, bank account opening, and so on.

Illegal provision: Some personal information can only cause significant risks to the rights and interests of the personal information subject because it is spread outside the authorized consent of the personal information subject, then it shall be determined as personal sensitive information. For example, sexual orientation, deposit information, history of infectious diseases, etc.

Abuse: When certain personal information is used beyond the reasonable limits of authorization (such as changing the processing purpose, expanding the processing scope, etc.), it may pose a significant risk to the rights and interests of the personal information subject and shall be determined as personal sensitive information. For example, when the authorization of the personal information subject is not obtained, the health information is used for the marketing of insurance companies and determining the level of individual premiums.

Table B.1 gives examples of personal sensitive information.

Appendix C

(Informative)

Method for realizing self-intention of personal information subject

C.1 Overview

The safeguarding of the personal information subject's autonomous will includes two aspects: one is not to force the personal information subject to accept multiple business functions; the second is to protect the personal information subject's right to know and consent to the collection and use of personal information. Personal information controllers, especially mobile Internet application operators, can be implemented in the following ways.

C.2 Distinguish between basic business functions and extended business functions

To protect the right of personal information subjects to choose to consent, first of all, it is necessary to divide the basic business function and extended business function of the product or service. The division method is as follows:

a) The basic business functions of the product or service shall be divided according to the fundamental expectations and the most important needs of the personal information subject to select and use the provided product or service;

Note 1: The reason why the personal information subject recognizes or selects a product or service is mainly based on the marketing and commercial positioning of the product or service provided by the personal information controller, the name of the product or service itself, the description in the application store, the type of application it belongs to and other factors. Therefore, the personal information controller shall, based on the most likely knowledge and understanding of the above factors by the general personal information subject, rather than their own ideas, determine the main needs and expectations of the personal information subject, to define the basic business functions. Generally speaking, if the product or service does not provide basic business functions, the personal information subject will not choose to use the product or service.

Note 2: With the iteration, expansion and upgrade of products or services, the basic business functions may need to be re-divided accordingly. The personal information controller can still redefine the basic business functions according to the most likely knowledge and understanding of the general personal information subject. But personal information controllers should not change the division of basic business functions and extended business functions within a short period of time. After the re-division, the personal information controller should inform and obtain the explicit

the interactive interface or design (such as pop-up window, text description, filled in box, prompt bar, prompt sound, etc.), to inform the personal information subject one by one of the provided extended business function and necessary personal information to be collected; allow personal information subjects to choose and agree to extended business functions item by item.

b) If the personal information subject does not agree to collect the personal information necessary for the extended business functions, the personal information controller shall not repeatedly seek the consent of the personal information subject. Unless the personal information subject actively chooses to enable the extended function, the number of requests for consent from the personal information subject shall not exceed one time within 48 hours.

c) If the personal information subject does not agree with the collection of personal information necessary for the extended business functions, it shall not refuse to provide basic business functions or reduce the service quality of basic business functions.

d) The interactive interface or design required by a) shall facilitate the personal information subject to access again and change the scope of the consent.

Note: The implementation method of the above requirements can refer to C.5.

C.5 Design of interactive functional interface

The personal information controller can refer to the template shown in Table C.1 to design an interactive functional interface, to ensure that the personal information subject can fully exercise his right to choose and agree.

This function interface shall, before the personal information controller starts collecting personal information, such as during product installation, or when the personal information subject uses the product or service for the first time, or when the personal information subject registers an account, be provided actively by the personal information controller to the personal information subject. If personal information is collected by filling in paper materials, the personal information controller can refer to the following template content to design the form, to ensure that the personal information subject can exercise the right to choose consent.

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

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