ICS 35.040
L80

National Standard of the People's Republic of China

GB/T 35273—2017

Information security technology - Personal information security specification

(Draft for Approval)
November 30, 2017

Released on December 29, 2017 Implemented on May 1, 2018

Issued by General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China and Standardization Administration of the People's Republic of China and Standardization Administration of the People's Republic of China

Table of Contents

Preface ····· III
Introduction ····· IV
1 Scope ····· 1
2 Normative References ····· 1
3 Terms and Definitions ····· 1
4 Basic Principles of Personal Information Security ····· 3
5 Collection of Personal Information ····· 4
5.1 Legitimacy Requirements for Collecting Personal Information ····· 4
5.2 Minimum Requirements for Collecting Personal Information ····· 4
5.3 Authorization of Collecting Personal Information ····· 4
5.4 Exceptions of Authorized Consent ····· 4
5.5 Explicit Consent to Collect Personal Sensitive Information ····· 5
5.6 Content and Publication of Privacy Policy ····· 5
6 Preservation of Personal Information ····· 6
6.1 Minimum time of keeping the personal information ····· 6
6.2 De-identification processing ····· 6
6.3 Transmission and Storage of Personal Sensitive Information ····· 6
6.4 Personal Information Controllers Stop Operation ····· 6
7 Use of Personal Information ····· 6
7.1 Personal Information Access Control Measures ····· 7
7.2 Display Restrictions of Personal Information ····· 7
7.3 Use limit of Personal Information ····· 7
7.4 Personal Information Access ····· 7
7.5 Personal Information Correction ····· 8
7.6 Personal Information Deletion ····· 8
7.7 Personal Information Subjects Withdraw Consent ····· 8
7.8 Personal Information Subjects Close the Account ····· 8
7.9 Personal Information Subjects Acquire the Personal Information Copy ····· 8
7.10 Automatic decision of constraint information system ····· 8
7.11 Responding to the request of the personal information subject ····· 9
7.12 Complaint Management ····· 9
8 Entrusted Processing, Sharing, Transfer and Public Disclosure of Personal Information ····· 9
8.1 Entrusted Processing ····· 9
8.2 Personal Information Sharing and Transfer ····· 10
8.3 Transfer of Personal Information in Acquisition, Merger and Reorganization ····· 10
8.4 Public disclosure of personal information ····· 10
8.5 Exceptions to Prior Authorization When Sharing, Transferring or Publicly Disclosing Personal Information ····· 11
8.6 Common Personal Information Controller ····· 11
8.7 Requirements for Cross-border Transmission of Personal Information ····· 11
9 Personal Information Security Incident Handling ····· 11
9.1 Emergency Handling and Report of Security Incident ····· 11
9.2 Notification of Security Incidents ····· 12
10 Management Requirements of the Organization ····· 12
10.1 Identification of Responsible Departments and Personnel ····· 12

10.2 Carry out Personal Information Security Impact Assessment ····· 12
10.3 Data Security Capability ····· 13
10.4 Personnel Management and Training ····· 13
10.5 Security Audit ····· 13
Appendix A (Informative Appendix) Personal Information Example ····· 15
Appendix B (Informative Appendix) Personal Sensitive Information Determination ····· 16
Appendix C (Informative Appendix) Methods to Guarantee the Right of Personal Information Subject to Choose Consent 17
Appendix D (Informative Appendix) Privacy Policy Template ····· 20
References ····· 29

Preface

This Standard was drafted according to the rules of GB/T 1.1-2009 *Directives for Standardization - Part 1: The Structure and Drafting of Standards*.

Please note that some content of this document may involve patents, and the document release agency does not assume responsibility for the identification of these patents.

This Standard is proposed and centralized in the National Information Security Standardization Technical Committee (SAC/TC260).

Drafting units of this Standard: Beijing Information Technology Security Evaluation Center, China Electronics Standardization Institute, Yixin Technology Co., Ltd., Sichuan University, Peking University, Tsinghua University, China Information Security Research Institute Co., Ltd., First Research Institute of the Ministry of Public Security, Shanghai Institute of International Studies, Alibaba (Beijing) Software Service Co., Ltd., Shenzhen Tencent Computer System Co., Ltd., Cyberspace GPEA Wall System Application Co., Ltd., Aliyun Cloud Computing Co., Ltd., Huawei Technologies Co., Ltd. And Qiangyun Data Technology Co., Ltd.

Main drafters of this Standard: Hong Yanqing, Qian Xiubin, He Yanzhe, Zuo Xiaodong, Chen Xingshu, Gao Lei, Liu Xiangang, Shao Hua, Cai Xiaodan, Huang Xiaolin, Gu Wei, Huang Jin, Shangguan Xiaoli, Zhao Zhangjie, Fan Hong, Du Yuejin, Yang Silei, Zhang Yanan, Jin Tao, Ye Xiaojun, Zheng Bin, Min Jinghua, Lu Chuanying, Zhou Yachao, Yang Lu, Wang Haizhou, Wang Jianmin, Qin Song, Yao Xiangzhen, Ge Xiaoyu, Wang Daokui, Zhao Ranran, Shen Xiyong.

Introduction

In recent years, with the rapid development of information technology and the popularization of Internet applications, more and more organizations collect and use a large number of personal information, bringing convenience to people's lives. At the same time, there are also problems such as illegal collection, abuse and disclosure of personal information, which seriously threaten the security of personal information.

This standard aims at the security problems of personal information and regulates the relevant behaviors of personal information controllers in information processing links such as the collection, preservation, use, sharing, transfer and public disclosure, aiming at curbing chaos such as illegal collection, abuse and leakage of personal information, and protecting the legitimate rights and interests of individuals and social public interests to the greatest extent.

If there are other provisions in laws and regulations on specific matters in the standards, such provisions shall be followed.

Information Security Technology and Regulations on Personal Information Security

1 Scope

This Standard regulates the principles and safety requirements to be followed in carrying out personal information processing activities such as the collection, preservation, use, sharing, transfer and public disclosure.

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

2 Normative References

The following documents are essential for the application of this document. For dated references, only the dated editions are applicable to this document. For undated references, the latest editions (including all amendments) are applicable to this document.

GB/T 25069-2010 Information Security Technology Terms

3 Terms and Definitions

Those defined in GB/T 25069-2010 and the following terms and definitions are applicable to this document.

3.1

Personal Information

All kinds of information recorded electronically or otherwise that can identify a specific natural person or reflect the activities of a specific natural person individually or in combination with other information.

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

Note 2: The scope and types of personal information can be found in Appendix A.

3.2

Personal Sensitive Information

Personal information that may endanger personal and property security, easily lead to damage to personal reputation, physical and mental health or discriminatory treatment, once disclosed, illegally provided or abused.

Note 1: Personal sensitive information includes identity document number, personal biometric information, bank account number, communication records and contents, property information, credit information, whereabouts track, accommodation information, health physiological information, transaction information, personal information of children under 14 years old (inclusive), etc.

Note 2: The scope and types of personal information can be found in Appendix B.

3.3

Personal Data Subject

Natural persons identified by personal information.

3.4

Personal Data Controller

Organizations or individuals that have the right to decide the purpose and method of personal information processing.

3.5

Collect

The act of obtaining control over personal information includes being actively provided by the personal information subject, automatically collected by interacting with the personal information subject or recording of the behavior of the personal information subject, and indirectly obtained by sharing, transferring and collecting public information.

Note: If the provider of products or services provides tools for the use of personal information subjects and the provider does not access personal information, it does not belong to the collection behavior mentioned in this standard. For example, if the offline navigation software does not return the user's location information to the software provider after the terminal obtains it, it does not belong to the personal information collection behavior.

3.6

Explicit Consent

The personal information subject makes a clear authorization for the specific processing of his personal information through written statements or active affirmative actions.

Note: Affirmative actions include personal information subjects actively making statements (in electronic or paper form), checking, clicking "agree", "register", "send", "dial", etc.

3.7

User Profiling

Through collecting, gathering and analyzing personal information, analyze or predict the personal characteristic model of a specific natural person, such as the occupation, economy, health, education, personal preferences, credit, behavior and other aspects to personal characteristic model.

Note: Direct use of the personal information of a specific natural person to form a characteristic model of the natural person is called direct user portrait. Using personal information other than a specific natural person, such as the data of its group, a characteristic model of the natural person is formed, which is called indirect user portrait.

3.8

Personal Information Security Impact Assessment

For personal information processing activities, the process of testing their legal compliance degree, judging various risks of damage to the legitimate rights and interests of personal information subjects, and evaluating the effectiveness of various measures used to protect personal information subjects.

3.9

Delete

It refers to the deletion of personal information in the system covering the daily business functions, so that it is kept not retrievable or accessible.

3.10

Public Disclosure

The act of disseminating information to society or unspecified groups.

3.11

Transfer Of Control

The process of transferring control of personal information from one controller to another.

3.12

Sharing

The process in which a personal information controller provides personal information to other controllers and both parties have independent control over personal information.

3.13

Anonymization

Through the technical processing of personal information, the personal information subject cannot be identified and the processed information cannot be restored.

Note: The information obtained after anonymization of personal information does not belong to personal information.

3.14

De-Identification

Through the technical processing of personal information, personal information subject can not be identified without the help of additional information.

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

4 Basic Principles of Personal Information Security

Personal information controllers should follow the following basic principles when carrying out personal information processing activities:

a) Principle of consistency of rights and responsibilities - to be responsible for the damage to the legitimate rights and interests of personal information subjects caused by their personal information processing activities.

b) Principle of clear purpose - possess legal, legitimate, necessary and clear personal information processing purpose.

c) Principle of choosing consent - express the purpose, method, scope and rules of personal information processing to the personal information subject and solicit its authorization and consent.

d) Principle of minimum adequacy - unless otherwise agreed with the personal information subject, only the minimum type and quantity of personal information required to meet the purpose authorized and agreed by the personal information subject are processed. After the purpose is achieved, personal information should be deleted in time according to the agreement.

e) Principle of openness and transparency - the scope, purpose, rules, etc. of dealing with personal information shall be disclosed in a clear, understandable and reasonable way, and external supervision shall be accepted.

f) Principle of ensuring security - possess the security capability matching the security risks faced, and take sufficient

management measures and technical means to protect the confidentiality, integrity and availability of personal information.

g) Principle of subject participation - provide personal information subjects with methods to access, correct, delete their personal information, withdraw their consent, cancel their accounts, etc.

5 Collection of Personal Information

5.1 Legitimacy Requirements for Collecting Personal Information

The requirements for the personal information controllers shall include:

a) To cheat, lure or force personal information subjects to provide their personal information is not allowed;
b) The function of products or services on collecting personal information shall not be concealed;
c) To obtain personal information from illegal channels is not allowed;
d) Personal information prohibited by laws and regulations shall not be collected.

5.2 Minimum Requirements for Collecting Personal Information

The requirements for the personal information controllers include:

a) The type of personal information collected should be directly related to the business function of realizing the product or service. Direct connection means that without the participation of this information, the functions of products or services cannot be realized.
b) The frequency of automatic collection of personal information should be the minimum frequency necessary to realize the business function of the product or service.
c) The amount of indirect access to personal information should be the minimum amount necessary to realize the business function of the product or service.

5.3 Authorization of Collecting Personal Information

The requirements for the personal information controllers include:

a) Before collecting personal information, the personal information subject should be clearly informed of the types of personal information collected by different business functions of the products or services provided, as well as the rules for collecting and using personal information (such as the purpose of collecting and using personal information, the method and frequency of collection, the storage area, the storage period, its own data security capability, the relevant information of external sharing, transfer and public disclosure, etc.), and obtain the authorization and consent of the personal information subject.
b) When obtaining personal information indirectly:
    1) The personal information provider shall be required to explain the source of personal information and confirm the legality of its personal information source.
    2) It is necessary to understand the scope of authorization and consent for personal information processing obtained by the personal information provider, including the purpose of use, whether the personal information subject is authorized to agree to transfer, share, public disclosure, etc. If the personal information processing activities required by the organization to carry out its business exceed the scope of the authorization, the explicit consent of the personal information subject shall be obtained within a reasonable period after obtaining the personal information or before processing the personal information.

5.4 Exceptions of Authorized Consent

Under the following circumstances, the personal information controller does not need to obtain the authorization and consent of the personal information subject to collect and use personal information:

a) Data directly related to national security and national defense security;
b) Data directly related to public security, public health, and major public interest;
c) Data directly related to criminal investigation, prosecution, trial and judgment execution;
d) For the purpose of safeguarding the life, property and other important legal rights and interests of the personal information subject or other individuals, which is difficult to obtain the consent of the subject;
e) Personal information subject that has been self-disclosed to the public by the subject of personal information;
f) The personal information collected from the information legally disclosed to the public, such as legal news reports, government information disclosure, etc.
g) It is necessary to sign and perform the contract according to the requirements of the personal information subject;
h) Information that is necessary to maintain the safe and stable operation of the provided products or services, such as the information that is for discovering and disposing of the failure of the products or services;
i) The personal information controller is a news unit and it is necessary for it to carry out legal news reports;
j) Personal information that is given de-identification treatment while providing academic research or description when research institution is used to carry out statistical or academic research based on the public interest;
k) Other circumstances stipulated in laws and regulations.

5.5 Explicit Consent to Collect Personal Sensitive Information

The requirements for the personal information controllers include:

a) When collecting personal sensitive information, the explicit consent of the personal information subject should be obtained. It should be ensured that the explicit consent of the personal information subject is a concrete, clear and definite expression of wish given voluntarily on the basis of full knowledge.
b) Before collecting personal sensitive information through active provision or automatic collection, you should:
    1) Inform the personal information subject of the core business functions of the products or services provided and the personal sensitive information that must be collected, and clearly inform the impact of refusing to provide or agree. Personal information subjects should be allowed to choose whether to provide or agree to automatic collection;
    2) If products or services provide other additional functions and need to collect personal sensitive information, what additional functions personal sensitive information is necessary to complete shall be explained to the personal information subject one by one before collection, and the personal information subject shall be allowed to choose item by item whether to provide or agree to automatically collect personal sensitive information. When the personal information subject refuses, it may not provide corresponding additional functions, but it should not be used as a reason to stop providing core business functions and the corresponding service quality should be ensured.

Note: The implementation method of the above requirements can be referred to Appendix C.

c) Before collecting the personal information of minors over 14 years old, the explicit consent of minors or their guardians shall be obtained; for under the age of 14, the explicit consent of his guardian shall be obtained.

5.6 Content and Publication of Privacy Policy

The requirements for the personal information controllers include:

a) Personal information controllers shall formulate privacy policies, which shall include but not be limited to:
    1) The basic information of the personal information controller, including the registered name, registered address, common office location and contact information of the relevant principle, etc.
    2) The purpose of collecting and using personal information and various business functions covered by the

purpose, such as using personal information to push commercial advertisements, using personal information to form direct user portraits and their uses, etc.

3) Personal information collected by each business function, as well as personal information processing rules such as collection method and frequency, storage area, storage period, etc. and the scope of personal information actually collected.
4) The purpose of sharing, transferring and publicly disclosing personal information, the types of personal information involved, the types of third parties receiving personal information, and the corresponding legal responsibilities undertaken.
5) The basic principles of personal information security to be followed, the data security capabilities to be possessed, and the personal information security protection measures to be taken.
6) The rights and realization mechanism of personal information subjects, such as access methods, correction methods, deletion methods, account cancellation methods, methods to withdrawal consent, methods of obtaining copies of personal information, methods of restricting automatic decision-making of information systems, etc.
7) The possible security risks after providing personal information and the possible impact of not providing personal information.
8) Channels and mechanisms for handling inquiries and complaints from personal information subjects, as well as external dispute resolution agencies and contact information.

b) The information disclosed by the privacy policy shall be true, accurate and complete.
c) The content of the privacy policy should be clear and easy to understand, conform to common language habits, using standardized numbers, illustrations, etc. and avoiding the use of ambiguous language, and provide a summary at the beginning to briefly describe the key points of the notification content.
d) Privacy policies should be publicly published and easy to access, for example, links should be set up in prominent positions such as the website homepage, mobile application installation page and social media homepage.
e) Privacy policies should be delivered to personal information subjects one by one. When the cost is too high or there are obvious difficulties, it can be issued in the form of announcement.
f) When the matters contained in a) of this article change, the privacy policy shall be updated in time and the personal information subject shall be re-informed.

Note: The privacy policy content can be referred to Appendix D.

6 Preservation of Personal Information

6.1 Minimum time of keeping the personal information

The requirements for the personal information controllers include:

a) The term of keeping the personal information shall be the shortest time required by realizing the purpose.
b) After exceeding the term of keeping personal information above, they shall delete the personal information or conduct the anonymous processing.

6.2 De-identification processing

After collecting personal information, the personal information controller should immediately carry out de-identification processing, and take technical and management measures to store the de-identification data and the information that can be used to restore and identify individuals separately, and ensure that individuals are not re-identified in subsequent personal information processing.

6.3 Transmission and Storage of Personal Sensitive Information

The requirements for the personal information controllers include:

a) When transmitting and storing personal sensitive information, security measures such as encryption should be adopted.

b) When storing personal biometric identification information, technical measures should be adopted to process it before the storage, for example, only a summary of personal biometric identification information should be stored.

6.4 Personal Information Controllers Stop Operation

When the personal information controller ceases to operate its products or services, it shall:

a) Timely stop the activities of continuing to collect personal information.

b) Notify the personal information subject of the notice of stopping operation in the form of one-by-one delivery or announcement.

c) Delete or anonymize the personal information they hold.

7 Use of Personal Information

7.1 Personal Information Access Control Measures

The requirements for the personal information controllers include:

a) For internal data operators authorized to access personal information, they should only access the minimum sufficient personal information and have the minimum data operation authority required by their duties according to the principle of minimum authorization.

b) It is appropriate to set up internal approval procedures for important operations of personal information, such as batch modification, copying and downloading.

c) The roles of safety management personnel, data operators and auditors should be set separately.

d) If it is really necessary to authorize specific personnel to process personal information beyond their authority due to work needs, it shall be approved by the person in charge of personal information or protection or the personal information organization and recorded in the book.

Note: For the determination of the person responsible for personal information protection or the personal information protection organization, refer to 10.1 of this Standard.

e) The behavior of accessing and modifying personal sensitive information should trigger operation authorization according to the requirements of business processes on the basis of the authority control of roles. For example, due to receiving a customer complaint, the complaint handler can only access the relevant information of the user.

7.2 Display Restrictions of Personal Information

For those involving the display of personal information through the interface (such as display screen and paper), the personal information controller should take measures such as de-identification of the personal information to be displayed, to reduce the risk of disclosure of personal information in the display process. For example, when displaying personal information, internal unauthorized personnel and other personnel other than the personal information subject are prevented from obtaining personal information without authorization.

7.3 Use limit of Personal Information

The requirements for the personal information controllers include:

a) Except for the purpose, when using personal information, clear identity orientation should be eliminated to avoid

accurate positioning of specific individuals. For example, in order to accurately evaluate the personal credit status, direct user portraits can be used, while indirect user portraits should be used for the purpose of pushing commercial advertisements.

b) If the information generated by processing the collected personal information can identify the personal identity of a natural person alone or in combination with other information, or reflect the personal activities of a natural person, it shall be identified as personal information. The handling should follow the scope of authorization and consent obtained when collecting personal information.

Note: If the personal information generated by processing belongs to personal sensitive information, the processing shall conform to the requirements of this Standard for personal sensitive information.

c) When using personal information, it shall not exceed the scope that is directly or reasonably related to the claimed purpose when collecting personal information. Due to business needs, if it is really necessary to use personal information beyond the above scope, the explicit consent of the personal information subject shall be obtained again.

Note: It is within the scope of reasonable connection with the purpose of collection to use the collected personal information for academic research or to obtain a description of the overall state of natural, scientific, social, economic and other phenomena. However, when providing the results of academic research or description to the outside, the personal information contained in the results should be de-identified.

7.4 Personal Information Access

The personal information controller shall provide the personal information subject with a method of accessing the following information:

a) The personal information or type it holds about the subject;

b) The source and purpose of the above personal information;

c) The identity or type of the third party that has obtained the above personal information.

Note: When a personal information subject proposes to access personal information that is not provided voluntarily, the personal information controller can make a decision on whether to respond and give an explanation after comprehensively considering the risks and damages that non-response may bring to the legitimate rights and interests of the personal information subject, as well as factors such as technical feasibility and cost of realizing the request.

7.5 Personal Information Correction

If the personal information subject finds that its personal information held by the personal information controller is wrong or incomplete, the personal information controller shall provide it with a method to request correction or supplement information.

7.6 Personal Information Deletion

The requirements for the personal information controllers include:

a) In accordance with the following circumstances, if the personal information subject requires deletion, the following personal information should be deleted in time:

   1) Personal information controllers collect and use personal information in violation of laws and regulations;

   2) The personal information controller collects and uses personal information in violation of the agreement with the personal information subject.

b) If the personal information controller violates the provisions of laws and regulations or violates the agreement with the personal information subject, and share or transfer personal information to a third party, and the personal

information subject requests deletion, the personal information controller shall immediately stop the sharing and transfer and notify the third party to delete it in time.

c) If the personal information controller publicly discloses personal information in violation of laws and regulations or the agreement with the personal information subject, and the personal information subject requests deletion, the personal information controller shall immediately stop the public disclosure and issue a notice requiring the relevant receiver to delete the corresponding information.

7.7 Personal Information Subjects Withdraw Consent

The requirements for the personal information controllers include:

a) Personal information subjects should be provided with methods to withdraw their consent authorization to collect and use their personal information. After withdrawing the consent, the personal information controller shall not process the corresponding personal information in the future.

b) The right of personal information subjects, to refuse to receive commercial advertisements pushed based on their personal information, should be guaranteed. To share, transfer and publicly disclose personal information to the outside, the personal information subject shall be provided with the method of withdrawing consent.

Note: Withdrawing consent does not affect the personal information processing based on consent before withdrawal.

7.8 Personal Information Subjects Close the Account

The requirements for the personal information controllers include:

a) Personal information controllers who provide services through registering accounts should provide personal information subjects with a method to cancel accounts, and the method should be simple and easy to operate.

b) After the personal information subject cancels the account, it should delete its personal information or anonymize it.

7.9 Personal Information Subjects Acquire the Personal Information Copy

According to the request of the personal information subject, the personal information controller shall provide the personal information subject with a method to obtain the following types of personal information copies, or directly transmit the following personal information copies to a third party if technically feasible:

a) Personal basic data and personal identity information;

b) Personal health physiological information and personal education work information.

7.10 Automatic decision of constraint information system

When decisions that significantly affect the rights and interests of the personal information subject are made only based on the automatic decisions of the information system (e.g. determining the personal credit and loan amount based on the user portrait, or using the user portrait for interview screening), the personal information controller shall provide the personal information subject with a complaint method.

7.11 Responding to the request of the personal information subject

The requirements for the personal information controllers include:

a) After verifying the identity of the personal information subject, the requests made by the personal information subject based on 7.4 to 7.10 of this Standard shall be responded in time, a reply and reasonable explanation shall be made within thirty days or within the time limit stipulated by laws and regulations, informing the personal

information subject of the way to propose dispute resolution to the outside.

b) In principle, there is no charge for reasonable requests, but for repeated requests within a certain period of time, a certain cost may be charged depending on the situation.

c) If it requires high cost or other obvious difficulties to directly realize the request of the personal information subject, the personal information controller should provide other alternative methods to the personal information subject to protect the legitimate rights and interests of the personal information subject.

d) The following circumstances may not respond to the requests made by the personal information subject based on 7.4 to 7.10 of this Standard, including but not limited to:
   1) Data directly related to national security and national defense security;
   2) Data directly related to public security, public health, and major public interest;
   3) Data directly related to criminal investigation, prosecution, trial and judgment execution;
   4) The personal information controller has strong evidence to prove that the personal information subject is subjectively malicious or abuses the right;
   5) Responding to the request of the personal information subject will cause serious damage to the legitimate rights and interests of the subject or other individuals and organizations;
   6) Data involving commercial secrets.

7.12 Complaint Management

Personal information controllers should establish a complaint management mechanism, including tracking procedures, and respond to complaints within a reasonable time.

8 Entrusted Processing, Sharing, Transfer and Public Disclosure of Personal Information

8.1 Entrusted Processing

When entrusting personal information, the following requirements shall be observed:

a) The entrustment of the personal information controller shall not exceed the scope of the authorization and consent of the personal information subject or comply with the provisions of 5.4 of this Standard.

b) The personal information controller shall carry out personal information security impact assessment on the entrusted behavior to ensure that the entrusted party has sufficient data security capability and provides sufficient security protection level.

c) The entrusted party shall:
   1) Handle personal information strictly according to the requirements of personal information controllers. If the entrusted party fails to process personal information according to the requirements of the personal information controller due to special reasons, it shall timely feedback to the personal information controller.
   2) If the entrusted party really needs to entrust again, he shall obtain the authorization of the personal information controller in advance.
   3) Assist the personal information controller to respond to the requests made by the personal information subject based on 7.4 to 7.10 of this Standard.
   4) If the entrusted party cannot provide sufficient security protection level or security incidents occur in the process of processing personal information, it shall timely feedback to the personal information controller.
   5) Personal information will no longer be saved when the entrustment relationship is dissolved.

d) The personal information controller shall supervise the entrusted party by means including but not limited to:
   1) Provisions on the responsibilities and obligations of the entrusted party through contracts and other means.
   2) Audit the entrusted party.

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

8.2 Sharing and Transfer of Personal Information

Personal information shall not be shared or transferred in principle. When personal information controllers really need to share and transfer, they should pay full attention to risks. Sharing and transferring personal information shall comply with the following requirements if it is not due to acquisition, merger or reorganization:

a) Carry out personal information security impact assessment in advance, and take effective measures to protect personal information subjects according to the assessment results.

b) Inform the personal information subject of the purpose of sharing and transferring personal information and the type of data receiver, and obtain the authorization and consent of the personal information subject in advance. Sharing or transferring the personal information with de-identification treatment and ensuring that the data receiver cannot re-identify the personal information subject is excepted.

c) Before sharing and transferring personal sensitive information, in addition to the contents notified in 8.2 b), the personal information subject shall also be informed of the type of personal sensitive information involved, the identity of the data receiver and the data security capability, and the explicit consent of the personal information subject shall be obtained in advance.

d) Accurately record and keep the sharing and transfer of personal information, including the date, scale and purpose of sharing and transfer, as well as the basic information of the data receiver, etc.

e) To bear the corresponding responsibility for the damage to the legitimate rights and interests of the personal information subject caused by the sharing and transfer of personal information.

f) To help the personal information subject understand the storage and use of personal information by the data receiver, as well as the rights of the personal information subject, such as accessing, correcting, deleting and canceling accounts.

8.3 Transfer of Personal Information in Acquisition, Merger and Reorganization

When the personal information controller changes such as acquisition, merger and reorganization, the personal information controller shall:

a) Inform the personal information subject of the relevant information.

b) The changed personal information controller shall continue to fulfill the responsibilities and obligations of the original personal information controller. For example, when the purpose of using personal information is changed, the explicit consent of the personal information subject shall be obtained again.

8.4 Public Disclosure of Personal Information

Personal information shall not be disclosed publicly in principle. When personal information controllers are authorized by law or have reasonable reasons that really need public disclosure, they shall pay full attention to risks and comply with the following requirements:

a) Carry out personal information security impact assessment in advance, and take effective measures to protect personal information subjects according to the assessment results.

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

c) Before publicly disclosing personal sensitive information, in addition to the contents disclosed in 8.4 b), the personal information subject shall also be informed of the contents of the personal sensitive information involved.

d) Accurately record and keep the public disclosure of personal information, including the date, scale, purpose and scope of public disclosure, etc.

e) To bear the corresponding responsibility for the damage to the legitimate rights and interests of the personal information subject caused by the sharing and transfer of personal information.

f) Personal biometric information shall not be publicly disclosed.

8.5 Exceptions to Prior Authorization When Sharing, Transferring or Publicly Disclosing Personal Information

Under the following circumstances, the personal information controller does not need to obtain the prior authorization and consent of the personal information subject to share, transfer and publicly disclose personal information:

a) Data directly related to national security and national defense security;

b) Data directly related to public security, public health, and major public interest;

c) Data directly related to criminal investigation, prosecution, trial and judgment execution;

d) For the purpose of safeguarding the life, property and other important legal rights and interests of the personal information subject or other individuals, which is difficult to obtain the consent of the subject;

e) Personal information that the personal information subject discloses to the public on its own;

f) The personal information collected from the information legally disclosed to the public, such as legal news reports, government information disclosure, etc.

8.6 Common Personal Information Controller

When the personal information controller and the third party are common personal information controllers (e.g., the service platform and the contracted merchants on the platform), the personal information controller shall jointly determine the personal information security requirements to be met with the third party through contracts and other forms, as well as the responsibilities and obligations to be assumed by himself and the third party respectively in terms of personal information security, and clearly inform them the personal information subject.

Note: Personal information controllers deploy third-party plug-ins to collect personal information in the process of providing products or services (e.g. website operators and deployment of statistical analysis tools, software development kit SDK, call map API interfaces in their web pages or applications). And the third party has not separately obtained the authorization to collect and use personal information from the personal information subject, the personal information controller and the third party are the common personal information controllers.

8.7 Requirements of Personal Information Cross-border Transmission

If the personal information collected and generated during the operation within the territory of the People's Republic of China is provided overseas, the personal information controller shall conduct security assessment in accordance with the measures and relevant standards formulated by the National Cyberspace Administration in conjunction with the relevant departments of the State Council, and meet its requirements.

9 Personal Information Security Incident Handling

9.1 Emergency Handling and Report of Security Incident

The requirements for the personal information controllers include:

a) Emergency plans for personal information security incidents should be formulated.

b) Relevant internal personnel shall be regularly (at least once a year) organized to carry out emergency response

training and emergency drills so that they can master job responsibilities and emergency disposal strategies and procedures.

c) After the occurrence of a personal information security incident, the personal information controller shall carry out the following disposal according to the emergency response plan:
   1) The record includes but is not limited to: the person, time and place where the incident was found, the personal information and number involved, the name of the system where the incident occurred, the impact on other interconnected systems, and whether the law enforcement agencies or relevant departments have been contacted.
   2) Assess the possible impact of the incident and take necessary measures to control the situation and eliminate hidden dangers.
   3) Report in timely according to the relevant provisions of the *National Network Security Incident Emergency Plan*, the report includes but is not limited to: type, quantity, content, nature and other overall information involving personal information subjects, the possible impact of the incident, the disposal measures taken or to be taken, and the contact information of relevant personnel involved in the incident disposal.
   4) According to the requirements of 9.2 of this Standard, the notification of security incident shall be implemented.
d) According to the changes of relevant laws and regulations, as well as the handling of incidents, update the emergency plan in time.

9.2 Security Incident Notification

The requirements for the personal information controllers include:

a) The affected personal information subjects should be informed of the relevant information of the incident in a timely manner by mail, letter, telephone, push notification, etc. When it is difficult to inform personal information subjects one by one, reasonable and effective ways should be adopted to issue warning information related to the public.
b) The content shall include but not limited to:
   1) Contents and impacts of security incidents;
   2) Disposal measures taken or to be taken
   3) Suggestions on self-prevention and risk reduction of personal information subjects;
   4) Remedial measures provided to personal information subjects;
   5) Contact information of the principle in charge of personal information protection and the personal information protection organization.

10 Management Requirements of the Organization

10.1 Identification of Responsible Departments and Personnel

The requirements for the personal information controllers include:

a) It should be clear that its legal representative or main principle shall take overall leadership responsibility for personal information security, including providing human, financial and material resources for personal information security work, etc.;
b) Principle in charge of personal information protection and the personal information protection organization shall be appointed;
c) Organizations that meet one of the following conditions shall set up full-time personal information protection principle and personal information protection agencies to be responsible for personal information security:
   1) The main business involves personal information processing, and the number of employees is more than 200.
   2) Processing the personal information of more than 500,000 people, or expected to process the personal

information of more than 500,000 people within 12 months.

d) The duties that the principle in charge of personal information protection and the personal information protection organization shall perform include but are not limited to:
   1) Fully coordinate the implementation of personal information security work within the organization, and bear direct responsibility for personal information security.
   2) Formulate, issue, implement and regularly update privacy policies and related regulations.
   3) Establish, maintain and update a list of personal information held by the organization (including the type, quantity, source, recipient, etc. of personal information) and authorized access policies.
   4) Carry out personal information security impact assessment.
   5) Organize and carry out personal information security training.
   6) Conduct the test before products or services are released online to avoid unknown collection, use, sharing and other processing behaviors of personal information.
   7) Conduct security audits.

10.2 Carry out Personal Information Security Impact Assessment

The requirements for the personal information controllers include:

a) Establish a personal information security impact assessment system, and regularly (at least once a year) carry out personal information security impact assessment.
b) The impact assessment of personal information security shall mainly assess the compliance of processing activities with the basic principles of personal information security and the impact of personal information processing activities on the legitimate rights and interests of personal information subjects, including but not limited to:
   1) Whether the personal information collection process follows the principles of clear purpose, choice of consent, minimum adequacy, etc.
   2) Whether the processing of personal information may adversely affect the legitimate rights and interests of the personal information subject, including whether the processing will endanger personal and property safety, damage personal reputation and physical and mental health, and lead to discriminatory treatment, etc.
   3) Effectiveness of personal information security measures.
   4) The anonymized or de-identified data set re-identifies the risks of the personal information subject.
   5) The possible adverse effects of sharing, transferring and publicly disclosing personal information on the legitimate rights and interests of personal information subjects.
   6) If a security incident occurs, it may have adverse effects on the legitimate rights and interests of personal information subjects.
c) When there are new requirements in laws and regulations, or when there are major changes in business models, information systems and operating environment, or when there are major personal information security incidents, the personal information security impact assessment shall be re-conducted.
d) Form a personal information security impact assessment report and take measures to protect the personal information subject, to reduce the risk to an acceptable level.
e) The personal information security impact assessment report shall be properly retained to ensure that it can be consulted by relevant parties and made public in an appropriate form.

10.3 Data Security Capability

Personal information controllers shall, in accordance with the requirements of relevant national standards, establish appropriate data security capabilities and implement necessary management and technical measures to prevent the leakage, damage and loss of personal information.

10.4 Personnel Management and Training

The requirements for the personal information controllers include:

a) A confidentiality agreement should be signed with relevant personnel engaged in personal information processing positions to conduct background checks on a large number of personnel who come into contact with personal sensitive information.
b) The safety responsibilities of different posts involved in personal information processing and the punishment mechanism for security incident should be clearly defined.
c) Relevant personnel in personal information processing positions shall be required to continue to perform their confidentiality obligations when transferring from their positions or terminating their labor contracts.
d) The personal information security requirements to be observed by external service personnel who may access personal information should be clearly defined, confidentiality agreements should be signed with them, and supervision should be carried out.
e) Professional training and assessment of personal information security shall be carried out, on a regular basis (at least once a year) or in the event of major changes in privacy policies, for relevant personnel in personal information processing positions, to ensure that relevant personnel are proficient in privacy policies and relevant procedures.

10.5 Security Audit

The requirements for the personal information controllers include:

a) Privacy policies and related procedures, as well as the effectiveness of security measures, should be audited.
b) An automated audit system should be established to monitor and record personal information processing activities.
c) The records formed in the audit process shall be able to provide support for the disposal, emergency response and post-event investigation of security incidents.
d) Unauthorized access, tampering or deletion of audit records shall be prevented.
e) Illegal use and abuse of personal information found during the audit should be dealt with in time.

Appendix A
(Informative Appendix)
Personal Information Example

Personal information refers to all kinds of information recorded electronically or otherwise that can identify a particular natural person individually or in combination with other information or reflect the activities of a particular natural person, such as name, date of birth, ID card, personal biometric information, address, contact information, communication log and content, account password, property information, credit investigation information, accommodation trajectory, accommodation information, health physiological information and transaction information.

To determine whether an item of information is personal information, the following two paths shall be considered: one is the identification, that is, from information to individuals, specific natural persons are identified by the particularity of the information itself. Personal information should be helpful to identify specific individuals. Second is the association, that is, from the individual to information, if a specific natural person is known, the information generated by the specific natural person in its activities (such as personal location information, personal phone records and personal browsing records) belongs to personal information. Information that meets either of the above circumstances shall be determined as personal information.

Table A.1 Personal Information Example

Basic personal information	Name, birthday, gender, ethnic group, nationality, family relationship, address, personal telephone number, e-mail, etc.
Personal identity information	ID card, military ID, passport, driving license, work permit, pass card, social security card, residence permit, etc.
Personal biological recognition information	Personal genes, fingerprints, vocal prints, palm prints, auricles, irises, facial recognition features, etc.
Network identity label information	System account, IP address, e-mail address, and password, command, command protection answer, user personal digital certificate, etc. related to the previous statement, etc.
Personal health physiological information	Records generated by illness and treatment, and other affairs, such as symptoms, hospital records, medical orders sheet, test reports, surgical and anesthetic records, nursing records, medication records, drug and food allergy information, fertility information, past medical history, diagnosis and treatment, family medical history, present medical history, history of infectious diseases, and information related to personal health status.
Personal education and work information	Personal occupation, position, work unit, educational background, degree, educational experience, work experience, training record, transcript, etc.
Personal property information	Bank account, authentication information (command), deposit information (including fund quantity, and payment and collection records), real estate information, credit records, credit investigation information, transaction and consumption records, daily records, and virtual property information such as virtual currency, virtual transaction and game redeem code.
Personal communication information	Communication log and content, SMS, MMS, e-mail, data describing personal communications (commonly referred to as metadata), etc.
Contact information	Address book, friend list, group list, e-mail address list, etc.
Personal access records	User operation records stored in the log, including website browsing records, software usage records, click records, etc.
Personal common equipment information	Information describing the basic information of a common personal device, including serial number of hardware, device MAC address, software list, and unique device identification code (such as IMEI/android ID/IDFA/OPENUDID/GUID, and IMSI information of SIM card)
Personal location information	Whereabouts, precise location information, accommodation information, longitude and latitude, etc.
	Marriage history, religious belief, sexual orientation, undisclosed criminal record, etc.

Appendix B
(Informative Appendix)
Personal Sensitive Information Determination

Personal sensitive information means the personal information that may endanger personal and property security, easily lead to damage to personal reputation, physical and mental health or discriminatory treatment, once disclosed, illegally provided or abused. Usually, personal information of children under 14 years of age and privacy information of natural persons are personal sensitive information, which can be determined from the following perspectives:

Disclosure: once personal information is disclosed, it will lead to the loss of control over personal information by the personal information subject and the organizations and institutions that collect and use personal information, leading to the uncontrollable diffusion and application of personal information. After disclosure, some personal information is directly used against the will of the personal information subject or is connectedly analyzed with other information, which may bring significant risks to the rights and interests of the personal data subject, and should be judged as personal sensitive information. For example, the photocopy of the identity card of the personal information subject is used for the real name registration of the mobile phone card, the bank account opening, card handling and so on.

Illegal supply: some personal information can bring significant risks to the rights and interests of the personal information subject only because it diffuses outside the scope of authorization and consent of the personal data subject, which should be judged as personal sensitive information. For example, sexual orientation, deposit information, history of infectious diseases, etc.

Abuse: the use of certain personal information beyond the reasonable limits of authorization (such as the purpose of change processing, expansion of processing scope, etc.) may pose a significant risk to the rights and interests of the personal information subject, such should be judged the personal sensitive information. For example, health information is used for marketing by insurance companies and determine individual premiums without authorization from the personal information subject.

Table B.1 Examples of Personal Sensitive Information

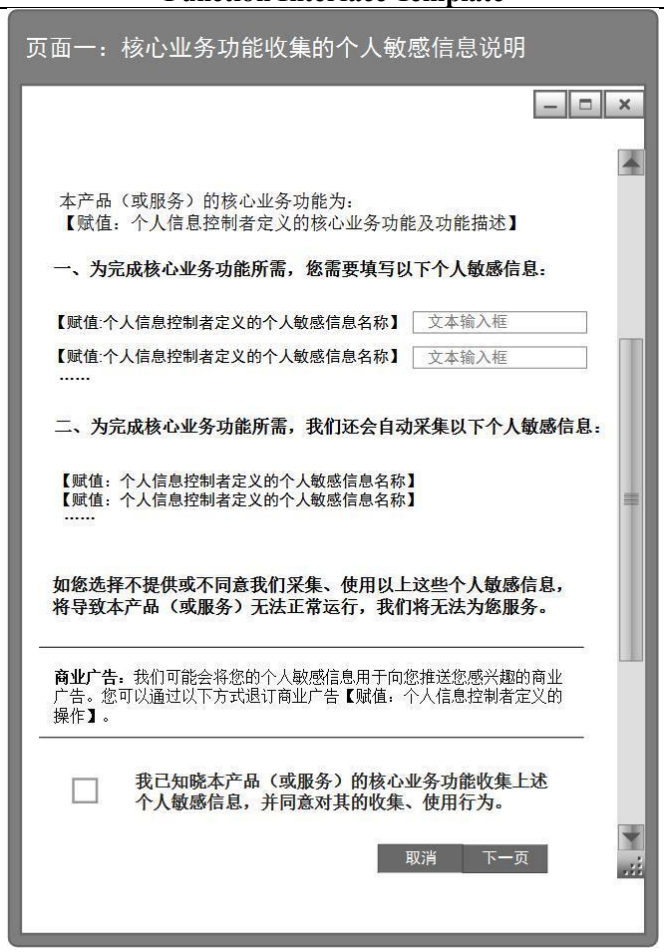
Table B.1 Personal Sensitive Information Example

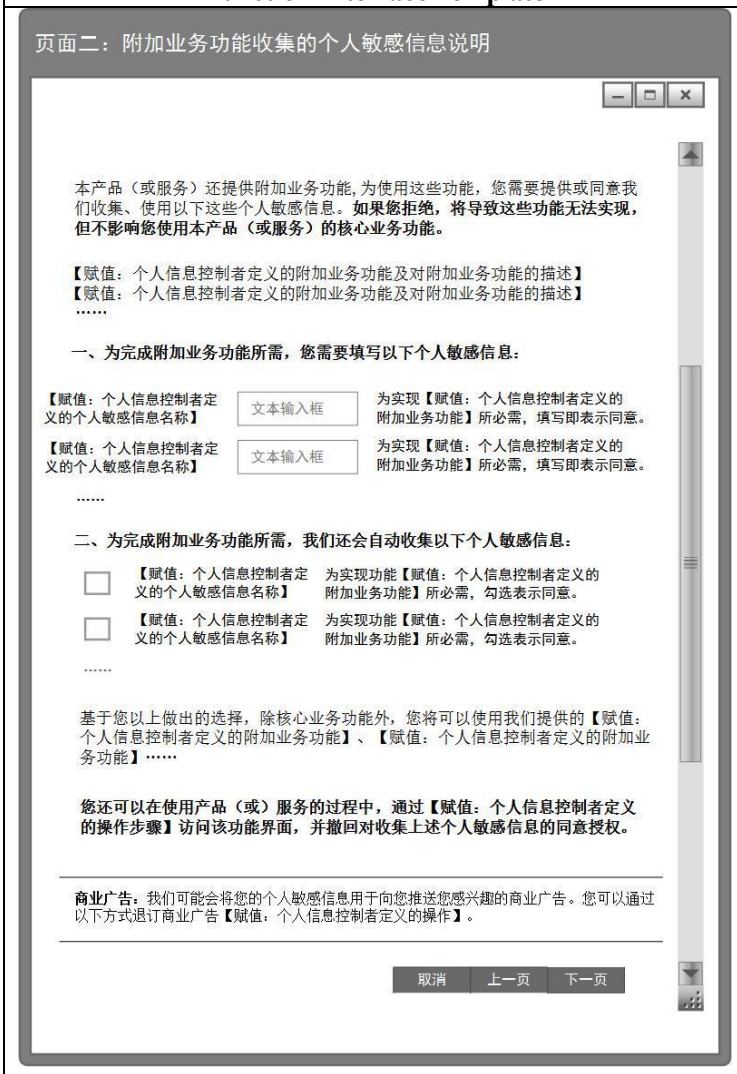
Personal property information	Bank account, authentication information (command), deposit information (including fund quantity, and payment and collection records), real estate information, credit records, credit investigation information, transaction and consumption records, daily records, and virtual property information such as virtual currency, virtual transaction and game redeem code.
Personal health physiological information	Records generated by illness and treatment, and other affairs, such as symptoms, hospital records, medical orders sheet, test reports, surgical and anesthetic records, nursing records, medication records, drug and food allergy information, fertility information, past medical history, diagnosis and treatment, family medical history, present medical history, history of infectious diseases, and information related to personal health status.
Personal biological recognition information	Personal genes, fingerprints, vocal prints, palm prints, auricles, irises, facial recognition features, etc.
Personal identity information	ID card, military ID, passport, driving license, work permit, social security card, residence permit, etc.
Network identity label information	System account, IP address, e-mail address, and password, command, command protection answer, user personal digital certificate, etc. related to the previous statement, etc.
Other information	Personal telephone number, sexual orientation, marriage history, religious belief, undisclosed criminal record, communication log and content, whereabouts, web browsing record, accommodation information, precise location information, etc.

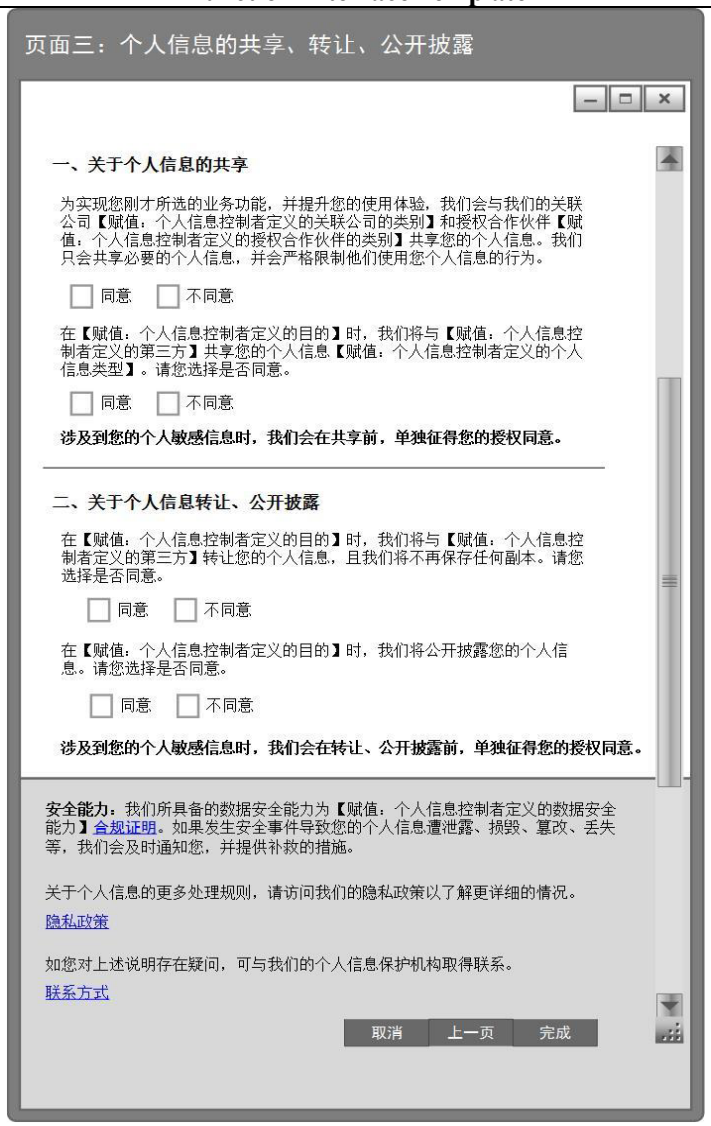
Appendix C
(Informative Appendix)
Methods to Guarantee the Right of Personal Information Subject to Choose Consent

This Appendix gives the implementation method of soliciting authorization and consent from personal information subjects on the collection and use of personal sensitive information, as well as the sharing, transfer and public disclosure of personal information. Personal information controllers can refer to the following templates to design functional interfaces to ensure that personal information subjects can fully exercise their right to choose and agree.

The function interface should be provided by the personal information controller to the personal information subject on its own initiative before the personal information controller starts to collect personal sensitive information, such as during the product installation process, or when the personal information subject uses the product or service for the first time, or when the personal information subject registers an account number. If personal sensitive information is collected by filling in paper materials, the personal information controller can refer to the following template content design form to ensure that the personal information subject can exercise the right to choose consent.

Function Interface Template	Description
	1. In order to clearly show the purpose and types of collecting personal sensitive information to the personal information subject, the consent of the personal information subject shall be obtained according to the situation. It is suggested that the personal information controller display the functional interface in the left template to the personal information subject in stages, windows and screens. 2. Personal information controllers need to clearly define the core business functions of their products (or services) and identify the personal sensitive information they must collect. 3. The assignment in the template on the left needs to be given by the personal information controller according to the actual situation, and the content should be clear and easy to understand. General and fuzzy statements are not allowed to describe the collected personal sensitive information. 4. The personal information controller can combine the actual product (or service) form and consider factors such as suitability and convenience to realize the functions in the left template. 5. When the personal information controller realizes the function interface on the left, the "check place" shall not be filled in in advance.

Function Interface Template	Description
	6. Additional business functions are other functions besides core business functions. Common additional business functions such as: Additional functions (such as voice recognition, picture recognition and geographic location) to improve the use experience of products (or services), additional functions to enhance the security mechanism of products (or services), etc. (such as collecting secret email boxes and fingerprints) 7. Additional business functions generally have the characteristics of selectivity, unsubscribing and not affecting core business. Personal information controllers need to fully analyze whether they have these characteristics when identifying additional business functions. Additional business functions shall not be equated with core business functions and to compulsorily collect personal sensitive information. 8. In this page, the personal information controller can display the additional functions available to the personal information subject in real time by integrating the personal sensitive information items voluntarily filled in by the personal information subject and the personal sensitive information items agreed to be automatically collected. 9. The personal information controller shall inform the personal information subject of the method of accessing the functional interface again to protect the right of the personal information subject to withdraw its consent.

Function Interface Template	Description
	10. Sharing, transferring and public disclosure with third parties may become diversified due to complex business functions. Personal information controllers may, at their discretion, add scenes of sharing, transfer and public disclosure on this page, or separately inform users in the form of pop-up windows and other forms during use, and obtain consent. 11. Data security capability refers to the ability of personal information controllers to protect the confidentiality, integrity and availability of personal information. Personal information controllers can prove their data security capability by carrying out relevant national standard compliance work, and display relevant certificates to personal information subjects in the form of links. 12. The personal information controller shall provide the personal information subject with a question-and-answer channel for the processing rules. If the personal information subject does not approve its processing rules, it may choose not to continue to use the product (or service). 13. The personal information subject shall be informed of the way to contact the personal information controller. 14. Links to privacy policies should be clearly indicated so that personal information subjects can consult them.

Appendix D
(Informative Appendix)
Privacy Policy Template

Publishing privacy policy is an important embodiment of personal information controllers' adherence to the principle of openness and transparency, an important means to ensure the information right of personal information subject, and an important mechanism to restrain their own behavior and cooperate with supervision and management. The privacy policy should offer clear, accurate and complete description of the personal information processing behavior of the personal data controller.

Privacy Policy Template	Compiling requirements
This policy applies only to XXXX products or services of XXXX, including... Last update date: MM/YYYY If you have any questions, comments or suggestions, please contact us at: Email: Tel.: Fax:	This section refers to the application scope, including the application scope of products or services for the privacy policy, user type, effective date, and the update time.
This policy will help you understand the following content: 1. The way we collect and use your personal information 2. How do we use Cookies and similar technologies 3. The way we share, transfer, and publicly disclose your personal information 4. The way we protect your personal information 5. Your rights 6. The way we handle children's personal information 7. The way your personal information transfers worldwide 8. The way to update this policy 9. The way you contact us XXXX is fully aware of the importance of personal information to you and will do its utmost to protect the security and reliability of your personal information. We are committed to maintaining your trust in us and to protecting your personal information in accordance with the following principles: consistency of powers and responsibilities, clarity of purpose, consent of choice, minimum adequacy, security, participation of subjects, transparency and so on. At the same time, XXXX promises to take appropriate security measures to protect your personal information in accordance with the industry's mature security standards. Please read and understand this Privacy Policy carefully before adopting our products (or services).	This section is a highlight of the privacy policy and an extract from the privacy policy. The purpose is to enable the personal information subject to quickly understand the main components of the privacy policy and the core of the statements made by the personal information controllers.

Privacy Policy Template	Compiling requirements
I. The way we collect and use your personal information Personal information means all kinds of information recorded electronically or otherwise that can identify a specific natural person or reflect the activities of a specific natural person individually or in combination with other information. XXXX will only collect and use your personal information for the following purposes described in this policy: **(I) Provide you with online shopping service** [Note: example] 1. Service function I: register as a user. To complete the creation of an account, you need to provide the following information: name, email address, user name and password you created... During the enrollment process, we will be able to provide you with better services and experiences if you provide the following additional information: mobile phone number, job title, company, education background... However, if you do not provide this information, it will not affect the basic service function of this service. The above information provided will continue to be licensed to us for the duration of your use of the service. When you cancel your account, we will stop using and delete the above information. The above information will be stored in the territory of the People's Republic of China. In case of cross-border transmission, we will obtain your authorization separately. 2. Service function II: commodity presentation, personalized recommendation, delivering promotion and marketing information. (Omitted) 3. Service function III: communicate with sellers. (Omitted) 4. Service function IV: payment and settlement. (Omitted) **(II) Delivery of products or services** [Note: example] (Omitted) **(III) Conduct internal audits, data analysis and research to improve our products or services** [Note: example] (Omitted) **(IV)...** ... Your prior consent will be sought when we intend to use the information for other purposes not specified in this policy. Your prior consent will be sought when we use the information gathered for a specific purpose for other purposes.	1. Provide a detailed list of the purposes for which personal information is collected and used, and do not use generic language. 2. List the types of personal information collected in detail according to the different service functions corresponding to the purpose. 3. Describe clearly which types of personal information are necessary for a particular service function. 4. When collecting information on legal documents and personal biological recognition information such as ID cards, passports, driving licenses, the personal information subject shall be specially reminded of the information involved in this collection, and the purpose and rules of processing shall be explained. 5. Do not use the generic language to summarize personal information collected, such as "we collect your identity and other related information", but should clearly state "we collect your name, phone number, and address information." 6. Describe the geographical area involved in the use of personal information, such as the area where personal information is stored and backed up, and the area involved in the transmission of personal information. If there is a cross-border transmission of personal information, a separate list or key identification is required. 7. When using personal information, whether or not to form a direct user portrait and its purpose need to be clearly stated. 8. In accordance with the usage of personal information, indicate the expected retention time of different types of personal information (e.g. 5 years from the date of collection) and the deadline for deletion or destruction (e.g. December 31, 2019 or when the user cancels the account). 9. Where there is a real need to change the purpose of information collection and use, it shall be stated that the consent of the user will be obtained.

Privacy Policy Template	Compiling requirements
II. How do we use Cookies and similar technologies **(I) Cookie** To ensure the normal working of website, we store a small data file called a Cookie on your computer or mobile device. Cookie typically contains identifiers, site names, and some numbers and characters. With the help of Cookie, websites can store data such as your preferences or items in a shopping basket. We will not use Cookie for any purpose other than those stated in this policy. You can manage or delete Cookie in accordance with your preferences. See AboutCookies.org for details. You can clear all Cookie saved on your computer and most web browsers have the ability to block Cookie. However in this way, you need to personally change your user settings when you visit our site. For more information on how to change browser settings, visit the following link: <Internet Explorer>, <Google Chrome>, <Mozilla Firefox>, <Safari>and <Opera>. **(II) Website beacons and pixel tags** In addition to Cookie, we use similar technologies such as website beacons and pixel tags on our websites. For example, the E-mail we sent you might contain a "click URL" that has the link to the content of our site. If you click on this link, we will track this click to help us understand your product or service preferences and improve customer service. A website beacon is usually a transparent image embedded in a website or E-mail. With the help of pixel tags in E-mail, we can know whether the e-mail is open or not. If you do not want your action to be tracked in this way, you can unsubscribe from our mailing list at any time. **(III) Do Not Track** Many web browsers have "Do Not Track" function, which publishes "Do Not Track" requests to websites. Currently, the major Internet standards bodies are not establishing policies on how websites should respond to such requests. But if your browser has enabled "Do Not Track", all of our websites will respect your choice. **(IV)...** ...	1. If a personal data controller or its authorized third party uses an automated data collection tool to collect personal information, a detailed description of the technical mechanisms used is required. 2. Common automated data collection tools are: Cookie, scripts, Web beacons, Flash Cookie, embedded Web links, local storage, etc. 3. Describe the purpose of using automated tools to collect personal information and provide users with methods and detailed guidance to limit the data collection of automated tools.

Privacy Policy Template	Compiling requirements
III. The way we share, transfer, and publicly disclose your personal information **(I) Sharing** We will not share your personal information with any company, organization, or individual other than XXXX except: 1. Share the information when receiving explicit consent: with your explicit consent, we will share your personal information with other parties. 2. We may share your personal information with the public in accordance with laws and regulations, or as mandatory requirements of the government authorities. 3. Share with our subsidiaries: your personal information may be shared with an affiliate of XXXX. We share only the necessary personal information which is bound by the stated purpose of this privacy policy. Your authorization will be sought again if the affiliates wish to change the purpose for processing of personal information. Our subsidiaries include: ... 4. Share with authorized partners: for the sole purpose stated in this policy, some of our services will be provided by authorized partners. We may share some of your personal information with our partners to provide better customer service and user experience. For example, when you buy our products online, we must share your personal information with our logistics service provider to arrange delivery or to arrange for partners to provide services. We will only share your personal information for legal, rightful, necessary, specific, and explicit purposes, and only share those required by the service. Our partners have no right to use the shared personal information for any other purpose. Currently, our authorized partners include the following X major types: 1) Authorized partners for advertising and analysis services. We will not share your Personal identity information (information that identifies you, such as your name or E-mail address, through which you can be contacted or identified) with partners that provide advertising and analysis services unless you allow us to do so. We provide these partners with information about their advertising coverage and effectiveness, rather than providing your personal identity information, or we aggregate this information so that it does not identify you personally. For example, only after the advertiser agrees to comply with our advertising guidelines, can we tell advertisers how effective their ads are, or how many people have seen their ads or installed apps after seeing ads, or provide these partners with personal information that can not identify the individual status (such as "25-year-old male in Beijing, likes software development") to help them understand their audiences or customers. 2) Suppliers, service providers and other partners. We send information to suppliers, service providers and other partners that support our business globally. These supports include providing technical infrastructure services, analyzing our service usage mode, measuring the effectiveness of advertising and services, providing customer service, convenience in payment or conducting academic research and surveys. 3)... We will enter into strict confidentiality agreements with companies, organizations, and individuals with whom we share personal information, requiring them to handle personal information in accordance with our instructions, this privacy policy, and any other relevant confidentiality and security measures. **(II) Transformation** We will not transfer your personal information to any company, organization or individual except: 1. Transfer the information when receiving explicit consent: with	1. Personal data controller explains whether sharing and transferring personal information is required, and describe in detail the type of personal information to be shared and transferred, the reasons for sharing and transferring personal information, the receiver of personal information, the constraints and management guidelines for the recipient, the purpose of using personal information by the recipient, the security measures in the process of sharing and transferring personal information, and whether sharing and transferring personal information poses a high risk to users. 2. The personal data controller shall explain whether the personal information needs to be disclosed publicly, and shall describe in detail the type, the reasons, and the possibility of the user of personal information and whether it would bring high risk to users. 3. Describe under which circumstances personal information controllers will share the transferred and publicly disclosed data without the consent of users, such as responding to requests from law enforcement agencies and government agencies, conducting personal information security audits, protecting users from fraud and serious bodily harm. 4. Description of responsibilities related to platform services. If the services provided by the personal data controller are platform services (e-commerce, social networking, information publishing, etc.), users need to be clearly reminded of the risks they face in uploading, communicating, publishing and sharing personal information, and state the security measures taken to share such information.

your explicit consent, we will transfer your personal information with other parties. 2. In the case of mergers, acquisitions or bankruptcy liquidations involving the assignment of personal information, we will require new companies and organizations holding your personal information to continue to be bound by this privacy policy, otherwise we will require such companies and organizations to seek your authorization again. **(III) Public disclosure** We will publicly disclose your personal information only if: 1. After obtaining your explicit consent; 2. Legal-based disclosure: we may disclose your personal information publicly where required by law, legal proceedings, litigation or mandatory requirements of government authorities.	

Privacy Policy Template	Compiling requirements
IV. The way we protect your personal information (I) We have used industry standard security precautions to protect your personal information from unauthorized access, public disclosure, use, modification, damage or loss of data. We will take all the reasonable and feasible measures to protect your personal information. For example, it is protected by SSL encryption when exchanging data, such as credit card information, between your browser and the "service". We also provide https security browsing mode for XXXX website, use encryption technology to ensure the confidentiality of data; use trusted protection mechanisms to protect our data from malicious attacks; deploy access control mechanisms to ensure that only authorized personnel have access to personal information. We will also provide training courses of security and privacy protection to strengthen employees' understanding about the importance of protecting personal information. (II) We have obtained the following certifications: ... (III) Our data security capabilities: ... (IV) We will take all the reasonable and feasible measures to ensure not to collect unrelated personal information. We will retain your personal information only within the time limit required for the purpose of this policy, unless the retention period has to be prolonged or it is permitted by law. (V) The Internet is not an absolutely secure environment, and e-mail, instant messaging and communication with other XXXX users are not encrypted. Therefore, we strongly recommend that you do not send personal information through such means. Please adopt complex passwords to help keep your account secure. (VI) We will regularly update and make public the relevant contents of the reports on security risks and personal information security impact assessments. You can get it by... (VII) Internet environment is not in 100% safety. We will try to ensure the safety of any information sent by you. If our physical, technical, or administrative safeguards are destroyed, resulting in unauthorized access to, public disclosure of, tampering or destruction of information, resulting in damage to your legitimate rights and interests, we shall be liable accordingly. (VIII) If security incident of personal information occurs unfortunately, we will timely notify you of the following matters in accordance with the requirements of laws and regulations: basic conditions and possible influence of security incident, disposal measures we have taken or are going to take, suggestions for your autonomous prevention and risk reduction, remedial measures for you, etc. We will promptly inform you of the relevant information by mail, letter, telephone, push notice or other means. When it is difficult to inform each personal information subject, we will take a reasonable and effective way to publish the announcement. Meanwhile, we will also take the initiative to submit the disposal conditions of personal information security incident in accordance with requirements of supervision department.	1. Describe in detail the measures taken by the personal data controller to protect the personal information, including, but are not limited to, personal information integrity protection measures, encryption measures for personal information transmission, storage and backup processes, personal information access, authorization and audit mechanisms for use, retention and deletion mechanisms for personal information, etc. 2. In accordance with the national standards such as GB/T AAAAA *Information Security Technology - Security Capacity Requirements for Big Data Services* and GB/T BBBBB *Information Security Techniques - Data Security Capacity Maturity Model*, we can determine our own data security capability. 3. The current personal information security protocols and the certification obtained, including the personal information security laws, regulations, standards, agreements which the personal information controller actively follows at present, as well as the personal information security-related authoritative and independent organization certification which the personal data controller has obtained at present. 4. Emphasis may be placed on reminding the public of how to protect their personal information when using products or services. 5. Security risks that may arise from the provision of personal information should be described. 6. It shall be indicated that the personal information controller shall bear legal liability after the occurrence of the personal information security incident. 7. It shall be indicated that the personal information subject will be notified in time after the occurrence of personal information security incident.

V. Your rights In accordance with the relevant laws, regulations, standards of China and the common practices of other countries and regions, we guarantee you the right to exercise the following rights with respect to your personal information: **(I) Access to your personal information** You have access right of your personal information, except for exceptional cases stipulated in laws and regulations. If you want to exercise data access, you can access it yourself by: Account information - if you want to access or edit profile and payment information in your account, change your password, add security information, or close your account, you can do so by accessing XXXX. Search information - you can access or clear your search history, view and modify interests, and manage other data in XXXX. ... If you cannot access this personal information through the links above, you can always contact us using our Web forms or send e-mail to XXXX. We will reply to your request for access within 30 days. We will provide you with any other personal information generated in the course of using our products or services, as long as we do not need to invest too much in it. If you want to exert the right of data access, please send e-mail to XXXX. **(II) Correct your personal information** You have the right to ask us to correct any errors you find in your personal information possessed by us. You can apply for corrections as in the way listed in "(I) Access to your personal information". If you cannot access this personal information through the links above, you can always contact us using our Web forms or send e-mail to XXXX. We will reply to your request for access within 30 days. **(III) Delete your personal information** You may make a request to us to delete personal information in the following circumstances: 1. we deal with personal information in violation of laws and regulations; 2. we collect and use your personal information without your consent; 3. we deal with personal information in violation of our agreement; 4. when you no longer use our products or services, or you cancel your account; 5. in case that we no longer provide you with products or services. If we decide to respond to your request for deletion, we will also notify entities that have obtained your personal information from us and require them to delete in time, unless otherwise provided by law or regulation, or if such entities are independently authorized by you. When you delete information from our service, we may not immediately delete the information in backup system, but we will delete it when we update the backup. **(IV) Change the scope of your authorization and consent** Each service function requires some basic personal information to be completed (see "Part I" of this policy). You may give or withdraw your authorization and consent at any time for the collection and use of additional personal information collected. You can do this as follows: ... When you withdraw your consent, we will no longer process the pertinent personal information. However, your decision to withdraw your consent will not affect any prior processing of personal information	1. Describe the rights owned by the user over his personal information, including but not limited to: selection scope of personal information available for users during the information collection, use and public disclosure; access, correction, deletion, acquisition and other control rights, user privacy preferences, communication and advertising preferences, access to consent withdrawal and account cancelation in case of service termination, the available channel for users to protect their rights and so on. 2. For purposes of access, correction, deletion, withdrawal of consent required configuration and operation (such as configuration and operation of software used, browser and mobile terminal) by oneself, the personal information controller shall specify the configuration and operation process in a manner that is easy for the user to understand, and when necessary, provide technical support channels (customer service phone, online customer service, etc.) 3. If costs incurred during the enforcement of rights by users, the reason and basis for charging shall be clearly stated. 4. In case that it takes a long time for the user to get response to the request for the enforcement of rights, specify the time node of the response and the reason why the response cannot be made in a short time. 5. When the user needs to verify his identity again during the enforcement of rights, the reasons for the verification shall be specified and appropriate control measure shall be taken to avoid the disclosure of personal information caused in the process of identity verification. 6. If the personal data controller refuses the user's request for access, correction, deletion, withdrawal of consent to the personal information, the reason and basis for the refusal shall be clearly stated.

based on your authorization. If you do not want to accept the commercial advertisements we send to you, you may cancel it at any time following these ways: ... **(V) Account cancellation by personal information subject** You can cancel your previously registered account at any time as follows: ... After canceling the account, we will stop providing you with products or services and delete your personal information upon your request, unless otherwise specified by laws and regulations. **(VI) Personal Information Subjects Acquire the Personal Information Copy** You have the right to obtain the copy of your personal information independently as follows: ...	

Privacy Policy Template	Compiling requirements
When technically feasible, such as data interface matching, we can also transmit a copy of your personal information directly to the third party you specified upon your request. **(VII) Automatic decision of constrain information system** With regard to some service functions, we may make decisions merely on the basis of non-manual automatic decision-making mechanisms such as the information system and algorithm. If these decisions significantly affect your legitimate rights and interests, you have the right to ask us for an explanation and we will provide appropriate remedies. **(VIII) Responding to your above requests** You may need to provide a written request or otherwise prove your identity to ensure your security. We may ask you to verify your identity before processing your request. We will reply within thirty days. If you are not satisfied, you can also complain through the following approaches: ... We do not charge you for reasonable requests in principle, but we will charge you for the costs depending on the conditions for repeated requests and the requests exceeding the reasonable limit. Requests for unwarranted duplication, requiring excessive technical means (for example, the development of new systems or radical changes to existing practices), posing risks to the legitimate rights and interests of others, or being highly impractical (for example, backing up information stored on tape), may be rejected. In the following cases, we cannot respond to your request in accordance with the requirements of laws and regulations: 1. data directly related to national security and national defense security; 2. data directly related to public security, public health, and major public interest; 3. data directly related to criminal investigation, prosecution, trial and judgment execution; 4. there is sufficient evidence that you have subjective malice or abuse of rights; 5. Responding to your request will cause serious damage to the legitimate rights and interests of you or other individuals and organizations. 6. Data involving commercial secrets.	

Privacy Policy Template	Compiling requirements
VI. The way we handle children's personal information Our product, website and service are mainly for adults. Children cannot create their own user accounts without the consent of parents or guardians. In case that we collect personal information of children with approval of parents or legal guardians, we will use or disclosure the data only in the condition permitted by the law, definitely approved by parents or guardians, or necessary condition of protecting children. Although local laws and customs have different definitions of children, yet we deem anyone below 14 years old as children. If we find ourselves having collected personal information of children without getting approval of provable parents in advance, we will try to delete related data as soon as possible.	
VII. The way your personal information transfers worldwide In principle, the personal information collected and generated within the territory of the People's Republic of China will be stored within the territory of the People's Republic of China. Since we provide products or services through resources and servers worldwide, this means that your personal information may be transferred to overseas jurisdictions in the countries/regions where you use the products or services upon receiving your authorized consent. Such jurisdictions may have independent data protection laws or maybe there is no related laws. In such cases, we will ensure that your personal information is adequately and protected equally within the territory of the People's Republic of China. For example, we ask for your consent to cross-border transfer of personal information or implement security measures such as de-identification before cross-border data transfer.	Where there is cross-border information transmission due to business needs, government and judicial regulatory requirements, the type of data to be transmitted across the border, as well as standards, protocols and legal mechanisms (contracts, etc.) to be observed for cross-border transmission shall be stated.
VIII. The way to update this policy Our privacy policy may change. However, we will not diminish your rights under this privacy policy without your explicit consent. Any changes to this policy will be posted on this page. We also provide more prominent notifications of material changes (including, for certain services, send e-mail notifications of specific changes to our privacy policy). Material changes referred to in this Policy include, but are not limited to: 1. Significant changes in our service model, such as the purpose of processing personal information, the type of personal information processed, the use of personal information and so on. 2. Major changes in our ownership structure and organizational structure, such as owner change arising from business restructuring, bankruptcy, mergers and acquisitions and so on. 3. Changes in main targets of personal information sharing, transfer or public disclosure. 4. Significant changes in your right to participate in the processing of personal information and the manner in which it is exercised. 5. Changes in responsible department, contact information and complaint channels for handling personal information security. 6. The personal information security impact assessment report indicates that there is a high risk. We will also archive older versions of this policy for your reference.	Personal information controllers are required to update their privacy policies in time when there is a material change in their policies and indicate how they will notify users in time. Typically, notification is given in the following ways: when users log in to the information system, the version of the information system is updated and a notification window pops up, when the user uses the information system, the notification is pushed directly to the users during the operation, and sends mail and SMS to the user, etc.

Privacy Policy Template	Compiling requirements
IX. The way you contact us If you have any questions, comments or suggestions regarding this privacy policy, please contact us by following ways: ... We set a dedicated personal information protection department (or personal information protection specialist) that you can contact by following ways: ... Normally, we will reply within thirty days. If you are not satisfied with our response, especially our personal information processing undermines your legitimate rights and interests, you may also seek solutions through the following external approaches: ...	1. Personal data controllers shall clearly provide relevant feedback and complaint channels for handling personal information security issues, such as contact information, address, e-mail address, user feedback form of the competent department of personal information security, and specify the time when users can receive responses. 2. The personal information controller shall provide the external dispute resolution provider and its contact information in response to disputes that cannot be settled through negotiation with the user. External dispute resolution providers are normally: courts in jurisdictions where personal information controllers is located, independent bodies, industry self-regulatory associations or relevant government regulatory bodies, etc. that certify personal data controllers' privacy policies.

References

[1] GB/T 32921-2016 Information Security Technology Information Technology Product Supplier Conduct Security Code

[2] GB/Z28828-2012 Information security technology Guidelines for the protection of personal information in public and commercial service information systems

[3] *Cybersecurity Law of the People's Republic of China* passed on the 24th Meeting of the Standing Committee of the 12th National People's Congress on November 7, 2016.

[4] The *Decision of the Standing Committee of the National People's Congress on Safeguarding Internet Security* passed on the 19th Meeting of the Standing Committee of the 9th Ninth National People's Congress on December 28, 2000.

[5] The *Decision of the Standing Committee of the National People's Congress on strengthening Internet information Security* passed on the 30th Meeting of the Standing Committee of the 11th Ninth National People's Congress on December 28, 2012.

[6] *Provisions on the Protection of Personal Information of Telecommunications and Internet Users* was released by the No. 24 Order of Ministry of Industry and Information Technology on July 16, 2013 and came into force since September 1, 2013.

[7] *Amendment to the Criminal Law of the People's Republic of China (VII)* passed on the 7th Meeting of the Standing Committee of the 11th National People's Congress on February 28, 2009.

[8] *Amendment to the Criminal Law of the People's Republic of China (IX)* passed on the 16th Meeting of the Standing Committee of the 12th National People's Congress on August 29, 2015.

[9] ISO/IEC 29100-2011 Information technology Security techniques Privacy framework

[10] EU General Data Protection Regulation 2015-05-24

[11] CWA 16113-2012 Personal Data Protection Good Practices

[12] ISO/IEC 29101-2013 Information technology Security techniques Privacy architecture framework

[13] NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organizations 2013-04

[14] NIST SP800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) 2010-04

[15] ISO/IEC FDIS 29134 Information technology Security techniques Privacy impact assessment 2017-02-20

[16] ISO/IEC FDIS 29151 Information technology Security techniques Code of practice for personally identifiable information protection 2016-12-16

[17] NISTIR 8062 An Introduction to Privacy Engineering and Risk Management for Federal Systems 2017-01

[18] ISO/IEC 2nd WD 29184 Information technology Security techniques Guidelines for online privacy notices and consent 2016-12-04

[19] EU-U.S Privacy Shield 2016-02-02

[20] The OECD Privacy Framework OECD 2013 [21] APEC Privacy Framework APEC 2005-12

[22] Consumer Privacy Bill of Rights Act of 2015 (Administration Discussion Draft) White House 2015-02