ICS 35.040
L80

National Standard of the People's Republic of China

GB/T 35273—2020
Replacing GB/T 35273-2017

Information security technology— Personal information (PI) security specification

信息安全技术 个人信息安全规范

(English Translation)

Issue date: 2020-03-06 Implementation date: 2020-10-01

Issued by State Administration for Market Supervision of the People's Republic of China
Standardization Administration of the People's Republic of China

Contents

Foreword III

Introduction IV

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Basic principles of PI security 4

5 PI collection 4

5.1 Lawfulness 4
5.2 Minimum necessary requirements 5
5.3 Independent choice among multiple business functions 5
5.4 Consent 5
5.5 PI protection policy 6
5.6 Exceptions to obtaining consent 7

6 PI storage 8

6.1 Minimization of storage time 8
6.2 De-identification 8
6.3 Transmission and storage of sensitive PI 8
6.4 Discontinuance of operation by PI Controllers 9

7 Use of PI 9

7.1 Access control measures 9
7.2 Restrictions on display 9
7.3 Restrictions on the purpose of use 10
7.4 Restrictions on the use of user profiling 10
7.5 Use of personalized display 11
7.6 Fusion of PI collected for different business purposes 11
7.7 Use of automatic decision-making mechanism of information systems 11

8 Rights of PI Subjects 12

8.1 Access 12
8.2 Rectification 12
8.3 Deletion 12
8.4 Withdrawal of consent 13
8.5 De-registration 13
8.6 Obtaining a copy of PI 14
8.7 Response to requests from PI Subjects 14
8.8 Complaint management 15

9 Entrusted processing, sharing, transfer and public disclosure of PI 15
9.1 Entrusted processing 15
9.2 Sharing and transfer 16
9.3 Transfer of PI in the case of acquisition, merger, reorganization or bankruptcy 17
9.4 Public disclosure 17
9.5 Exceptions to obtaining consent prior to the sharing, transfer or public disclosure of PI 18
9.6 Common controllers of PI 18
9.7 Third-party access management 18
9.8 Cross-border transfer 19
10 Handling of PI security incidents 19
10.1Emergency handling and reporting of PI security incidents 19
10.2 Notification of PI security incidents 20
11 PI security management requirements for organizations 20
11.1 Specifying responsible department and person 20
11.2 PI security engineering 21
11.3 Records of PI processing activities 22
11.4 PI security impact assessment 22
11.5 Data security capabilities 23
11.6 Personnel management and training 23
11.7 Security audit 23
Annex A (Informative) Examples of personal information 25
Annex B (Informative) Identification of sensitive personal information 27
Annex C (Informative) Methods to safeguard independent choice of personal information subject 29
Annex D (Informative) Personal information protection policy template 34
Bibliography 41

Foreword

SAC/TC 260 is in charge of this English translation. In case of any doubt about the contents of English translation, the Chinese original shall be considered authoritative.

This document is drafted in accordance with the rules of GB/T 1.1-2009.

This document replaces GB/T 35273-2017 Information security technology-Personal information security specification. In addition to a number of editorial changes, the following technical revisions have been made with respect to GB/T 35273-2017 (the previous edition).

— “Independent choice among multiple business functions” (5.3) has been added;
— “Exceptions to obtaining consent” (5.6 in this document and 5.4 in the 2017 version) has been modified;
— “Restrictions on the use of user profiling” (7.4) has been added;
— “Use of personalized display” (7.5) has been added;
— “Fusion of PI collected based on different business purposes” (7.6) has been added;
— “De-registration by personal information subject” (8.5 in this document and 7.8 in the 2017 version) has been modified;
— “Third-party access management” (9.7) has been added;
— “Specifying responsible department and person” (11.1 in this document and 10.1 in the 2017 version) has been modified;
— “Personal information security engineering” (11.2) has been added;
— “Records of personal information processing activities” (11.3) has been added;
— “Methods to safeguard independent choice of personal information subject” (Annex C in both this document and the 2017 version) has been modified.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuing body of this document shall not be held responsible for identifying any or all such patent rights.

This document was proposed and prepared by SAC/TC 260 (the National Information Security Standardization Technical Committee).

The previous editions replaced by this document are as follows:
GB/T 35273—2017.

Introduction

In recent years, with the rapid development of information technology and the popularization of Internet applications, more and more organizations are collecting and using personal information. At the same time as the public enjoy the convenience brought by technologies, the illegal collection, abuse and leakage of personal information are posing serious threats to personal information security.

In accordance with the Cybersecurity Law of the People’s Republic of China, this document focuses on the security issues of personal information, and standardizes information controllers’ behaviors at various stages of information processing, including the collection, storage, use, sharing, transfer and public disclosure of personal information, so as to stem the illegal collection, abuse and leakage of personal information and protect the legitimate rights and interests of individuals and public interests to the greatest extent possible.

Where laws and regulations provide otherwise, such provisions shall prevail.

Information security technology-Personal information (PI) security specification

1 Scope

This document specifies the principles and security requirements for the collection, storage, use, sharing, transfer, public disclosure and deletion of PI.

This document is applicable to PI processing activities carried out by all kinds of organizations. The document can also be used by competent authorities, third party assessment agencies and other organizations to supervise, manage and evaluate PI processing activities.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 25069—2010 *Information security technology – Terminology*

3 Terms and definitions

For the purpose of this document, the terms and definitions given in GB/T 25069-2010 and the following apply.

3.1
personal information
PI

any information that is recorded, electronically or otherwise, that can be used alone or in combination with other information to identify a natural person or reflect the activity of a natural person

Note 1 to entry: PI includes the name, date of birth, ID number, personal biometric information, residential address, contact information, communication records and content, username and password, property information, credit information, records of whereabouts, accommodation information, health and physiological information, transaction information of an individual.

Note 2 to entry: See Annex A for identification methods and types of PI.

Note 3 to entry: Information, such as user profiling or feature or labels, that results from PI controller's processing of PI or other information and can be used alone or in combination with other information to identify a particular natural person or reflect the activity of a particular natural person, is also deemed PI.

3.2

sensitive PI

PI that once leaked, illegally provided or abused, could endanger personal and property safety, or easily lead to damages to personal reputation, mental & physical health, or discriminatory treatment, etc.

Note 1 to entry: Sensitive PI includes ID numbers, personal biometric information, bank account information, communication records and content, property information, credit information, records of whereabouts, accommodation information, health information, transaction information, and the PI of minors up to 14 years of age.

Note 2 to entry: See Annex B for identification methods and types of sensitive PI.

Note 3 to entry: Information resulting from PI Controller's processing of PI or other information, that once leaked, illegally provided or abused could endanger personal and property safety, or easily lead to damages to personal reputation, physical & mental health, or discriminatory treatment, etc., is also deemed sensitive PI.

3.3

PI Subject

natural person identified by or associated with PI

3.4

PI Controller

organization or person that is in a position to determine the purpose, means, etc. of PI processing

3.5

collection

act of obtaining control of PI

Note 1 to entry: Including the act of automatically collecting PI such as accepting the PI volunteered by PI Subjects, obtaining PI by interacting with PI Subjects or by recording the behavior of PI Subjects, and the act of indirectly obtaining PI through sharing, transferring, collecting publicly available information, etc.

Note 2 to entry: Where a product or service provider provides a tool for PI Subjects to use, but the provider does not access the PI collected by the tool, the situation is not deemed an act of collection for the purpose of this document. For example, if an offline navigation software on a terminal obtains a PI Subject's location information, if the software does not transmit the information back to the software provider, then the situation is not deemed an act of collection for the purpose of this document.

3.6

explicit consent

act whereby a PI Subject explicitly authorizes the specific processing of his/her PI by making a written statement, including by electronic means, or an oral statement, or by making an affirmative action of his/her own accord

Note 1 to entry: Affirmative action includes situations where a PI Subject checks or clicks "agree", "register", "send", "dial", fills in a form, or provides his/her PI of his/her own accord.

3.7

consent

act whereby a PI Subject expressly authorizes the specific processing of his/her PI

Note 1 to entry: Including authorization through a positive act (i.e., explicit consent) or through a passive act (e.g., a PI Subject in the information collection area has not left the area after being informed that his/her information was going to be collected.

3.8

user profiling

process of analyzing, predicting and modeling the personal characteristics of a particular natural person, such as his/her occupation, financial status, health status, education, personal preferences, credit records and behavior by collecting, gathering and analyzing his/her PI

Note 1 to entry: Directly using a natural person's specific PI to model the characteristics of the natural person is called *direct user profiling*. Using the PI other than that of a specific natural person, such as the data of the group to which the natural person belongs, to model the characteristic of the natural person, is called *indirect user profiling*.

3.9

PI security impact assessment

process to check the degree of compliance with laws and regulations of PI processing activities, determine the potential risks to the legitimate rights and interests of PI Subjects, and assess the effectiveness of the measures used to protect PI Subjects

3.10

delete

act of removing PI from the system performing day-to-day business functions to keep it irretrievable and inaccessible

3.11

public disclosure

act of releasing the information to the public or to a non-specific group

3.12

transfer

process of moving the control of PI from one controller to another

3.13

sharing

process by which a PI Controller provides PI under its control to another PI Controller, resulting in each party having independent control over the PI

3.14

anonymization

irreversible technical process that makes PI Subjects unidentifiable or unassociated

Note 1 to entry: Anonymized PI is no longer deemed PI.

3.15

de-identification

technical process that makes PI Subjects unidentifiable or unassociated without the help of additional information

Note 1 to entry: De-identification is individually based and maintains the data granularity. It uses pseudonyms, encryption, hash functions and other technical means to replace the personal identifiers.

3.16
personalized display

activity of displaying information or providing search results for products or services to PI Subjects based on their PI, including their web browsing history, interests, consumption records and habits

3.17
business function

service types that meet the specific needs of PI Subjects

Note 1 to entry: E.g., map & navigation service, online car hailing, instant messaging, online community, online payment, news & information, online shopping, express delivery, and transport ticketing

4 Basic principles of PI security

PI Controllers, in carrying out PI processing activities, shall follow the principles of lawfulness, justification and necessity. Specifically, these include:

a) Balancing rights with responsibilities. PI Controllers shall take technical and other measures necessary to safeguard the security of PI, and be held accountable for harms to the legitimate rights and interests of PI Subjects caused by their PI processing activities.

b) Clear purpose. PI Controllers shall have an unequivocal, clear and specific purpose in processing PI.

c) Consent. PI Controllers shall explicitly inform PI Subjects of the purpose, method, scope and other rules for PI processing, and seek the PI Subjects' consent.

d) Minimum necessary. PI Controllers shall only process the minimum amount of information essential to meeting the purpose that the PI Subject has consented to. After the purpose is fulfilled, the PI shall be deleted promptly.

e) Transparency. PI Controllers shall publicly disclose the scope, purpose and rules, inter alia, for PI processing in a clear, understandable and reasonable manner, and accept external supervision.

f) Security. PI Controllers shall possess security capabilities that match potential security risks and adopt adequate administrative and technical measures to protect the confidentiality, integrity, and availability of PI.

g) Participation of PI Subjects. PI Controllers shall provide PI Subjects with channels to access, rectify, and delete their PI, as well as to withdraw consent, de-register, lodge a complaint, etc.

5 PI collection

5.1 Lawfulness

PI Controllers shall not:

a) collect PI through deception, inducement, or misinformation;

b) conceal the PI collection function of their products or services; or

c) obtain PI from illegal channels.

5.2 Minimum necessary requirements

Requirements on PI Controllers include:

a) The types of PI collected shall be directly related to the fulfillment of a product or service's business functions. "Directly related" means that the function of the product or service cannot be fulfilled without the above-mentioned PI.

b) The frequency of automatic PI collection shall be minimally necessary for the fulfillment of the business function of a product or service.

c) The amount of PI indirectly obtained shall be minimally necessary for the fulfillment of the business function of a product or service.

5.3 Independent choice among multiple business functions

When a product or service provides a number of business functions that require the collection of PI, the PI Controller shall not force PI Subjects to accept the business functions provided by the product or service and the corresponding requests for PI collection. Requirements on the PI Controller include:

a) The PI Controller shall not, by bundling the business functions of a product or service, require PI Subjects to accept and give bulk consent to requests for PI collection for the business functions that the PI Subjects have not used or applied for;

b) The PI Controller shall take the affirmative action by PI Subjects, such as proactive clicking, ticking, and filling-in, as the condition for activating a specific business function of a product or service. The PI Controller shall only initiate the collection of PI after the PI Subjects have activated the business function;

c) The PI Controller shall make the path or method for PI Subjects to deactivate or exit from a business function as convenient as the one for the PI Subjects to opt in for such business function. After the PI Subjects choose to deactivate or exit from a particular business function, the PI Controller shall stop the PI collection for such business function;

d) Where a PI Subject has not authorized the use of, deactivated or exited from a particular business function, the PI Controller shall not frequently request consent from the PI Subject;

e) Where a PI Subject has not authorized the use of, deactivated or exited from a particular business function, the PI Controller shall neither suspend any other business function for which the PI Subject has opted in voluntarily nor reduce the service quality of any other business function;

f) The PI Controller shall not demand the PI Subjects to authorize the collection of PI only for the purposes of raising service quality, improving user experience, developing new products or enhancing security.

5.4 Consent

Requirements on PI Controllers include:

a) When collecting PI, PI Controllers shall inform PI Subjects of the purpose, method, scope and other rules for collecting and using such PI, and obtain consent from the PI

Subjects;

Note 1: If a product or service only provides one business function that collects and uses PI, the PI Controller may inform the PI Subjects by way of a PI protection policy; if a product or service provides several business functions that collect and use PI, the PI Controller should, in addition to the providing the PI protection policy, inform the PI Subjects of the purpose, method and scope of the collection and use of such PI when starting to collect particular PI so that the PI Subjects can thoroughly consider the specific impact before giving consent.

Note 2: See Annex C for the implementation method that meets the requirements set in 5.3 and 5.4 a).

b) Before the collection of sensitive PI, the PI Controllers shall obtain explicit consent from the PI Subjects. The explicit consent shall be a specific and clear expression of intention voluntarily made by the PI Subjects on the basis of complete knowledge;

c) Before the collection of personal biometric information, the PI Controllers shall inform the PI Subjects separately of the purpose, method, scope, storage time and other rules for collecting and using such information and obtain explicit consent from the PI Subjects;

Note 3: Personal biometric information includes genes, fingerprints, voice prints, palm prints, auricles, iris and facial recognition features.

d) Before the collection of PI of minors at 14 years old and above, the PI Controllers shall obtain explicit consent from the minors or their guardians; for minors under 14 years old, explicit consent from their guardians is required;

e) In the case of indirect acquisition of PI:

   1) The PI Controller shall require the PI provider to explain the source of the PI, and verify the lawfulness of such source;

   2) The PI Controller shall understand the scope of consent the PI provider has obtained for processing the PI, including the purpose of use, and whether the PI Subjects have authorized the transfer, sharing, public disclosure and deletion of such information;

   3) If the PI processing activity required by the business goes beyond the scope of consent obtained, the PI Controller shall obtain explicit consent from the PI Subjects either by itself or through the PI provider within a reasonable time after the acquisition of the PI or before the processing of such information.

5.5 PI protection policy

Requirements on PI Controllers include:

a) The PI Controllers shall develop a PI protection policy that includes but is not be limited to the following content:

   1) Basic information about the PI Controller, including the identity and contact information;

   2) Business functions that collect and use PI, and the types of PI each of the business functions collects. Where sensitive PI is involved, relevant content shall be explicitly marked or highlighted;

   3) The collection method and storage period of PI, whether cross-border data transfer is involved, and other PI processing rules;

4) Purposes of the sharing, transfer and public disclosure of PI, the types of PI involved, the types of third parties receiving the PI, and respective security and legal responsibilities;

5) Rights of PI Subjects and implementation mechanisms, such as methods to access, rectify or delete their PI, to de-register, withdraw consent, obtain a copy of their PI, and to lodge a complaint about the automated decisions by information systems;

6) Security risks after consenting to PI collection, and possible impacts of not consenting to ant PI collection;

7) The basic principles of PI security followed, the data security capabilities in place, and the PI security protection measures adopted; compliance certificates related to data security and PI protection may be disclosed when necessary;

8) Channels and mechanisms for handling the inquiries and complaints of PI Subjects, and external dispute settlement agencies and their contact information.

b) Information contained in the PI protection policy shall be truthful, accurate and complete;

c) The PI protection policy shall use common language that is easily understandable, use standard figures & diagrams, and avoid ambiguous language;

d) The PI protection policy shall be publicly released and easily accessible, for example, through a link placed prominently on a homepage, an installation page of a mobile-Internet application (APP), or an interface or interactive design under Annex C;

e) The PI protection policy shall be served to each and every PI Subject. Where the costs are too high or there are significant difficulties, the policy may be released in the form of a public notice;

f) If any information included in a) changes, the PI Controllers shall update the PI protection policy promptly and notify the PI Subjects.

Note 1: An organization may continue to use “privacy policy” or other names for PI protection policy, but the content shall be consistent with that of the PI protection policy.

Note 2: See Annex D for the content of a PI protection policy.

Note 3: When a PI Subject activates a product or service for the first time or registers for an account, the main or core content of the PI protection policy should be displayed to the PI Subject through a pop-up window or in other forms to help the PI Subject understand the scope of and rules for PI processing of the product or service before deciding whether to use such product or service.

5.6 Exceptions to obtaining consent

In the following cases, the PI Controller does not have to obtain consent from the PI Subjects for collecting and using their PI:

a) In connection with the fulfilment of obligations under laws and regulations by the PI Controller;

b) Directly related to national security or national defense;

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

d) Directly related to criminal investigations, prosecutions, trials or execution of court decisions;

e) For the purpose of safeguarding the life, property or other significant legitimate rights and interests of the PI Subjects or other individuals, and it is hard to obtain consent from the PI Subjects;

f) The PI involved is disclosed to the public by the PI Subject;

g) (The collecting and using of PI are) essential to the signing and performing of a contract requested by the PI Subject;

   Note 1: The main function of the PI protection policy is to disclose the scope of and rules for the PI Controllers' collection and use of PI, therefore it should not be deemed a contract.

h) The PI is collected from legally and publicly disclosed information, such as legal news reports and government information disclosure;

i) (The collecting and using of PI are) essential to maintaining safe and stable operation of the product or service provided, such as the discovery and handling of product or service failures;

j) The PI Controller is a news agency and the collecting and using of PI are essential for it to carry out legitimate news reporting;

k) The PI Controller is an academic research institution and the collecting and using of PI are essential for it to carry out statistics or academic research for public interests, provided that the PI contained in the results is de-identified when it makes the academic research or the descriptive results available.

6 PI storage

6.1 Minimization of storage time

Requirements on PI Controllers include:

a) The storage time for PI shall be limited to the shortest time possible required for achieving the purpose of use consented to by the PI Subject, unless otherwise stipulated by laws and regulations, or otherwise consented to by the PI Subject;

b) The PI shall be deleted or anonymized after the above-mentioned storage time limit for PI.

6.2 De-identification

The PI Controllers should de-identify the PI immediately after collection, and take technical and management measures to store separately the information enabling the restoration of PI and the de-identified information, and enhance access and use management.

6.3 Transmission and storage of sensitive PI

Requirements on PI Controllers include:

a) The PI Controllers shall employ encryption and other security measures for the transmission and storage of sensitive PI;

   Note 1: Relevant national standards for cryptographic management should be complied with when adopting encryption technologies.

b) Personal biometric information and personal identity information shall be stored separately;

c) The PI Controllers shall not store the original personal biometric information (such as specimen and images) in principle. Measures that could be taken include but are not limited to:
   1) Storing only the summary information of personal biometric information;
   2) Enabling functions such as identification and authentication to be completed with personal biometric information on the terminal that collects such information;
   3) After the functions such as identification and authentication are completed with facial recognition features, fingerprints, palm prints, iris patterns and the likes, deleting the original image from which the personal biometric information could be extracted.

   Note 2: The summary information is often irreversible and cannot be used to retrieve the original information.

   Note 3: Cases where the PI Controller carries out its obligations stipulated by laws and regulations are excluded.

6.4 Discontinuance of operation by PI Controllers

The PI Controllers shall, in the case of discontinuance of operation of a product or service:

a) Stop collecting PI in a timely fashion;
b) Notify PI Subjects of the discontinuance of operation by sending a notice to each of them or through a public notice;
c) Delete or anonymize the PI they hold.

7 Use of PI

7.1 Access control measures

Requirements on PI Controllers include:

a) The PI Controllers shall establish a minimum access control policy for the personnel with authorized access to PI, so that they could only access minimized PI necessitated by their duties and have minimized data operation authorization to fulfill their duties;
b) The PI Controllers shall establish an internal approval process for important operations regarding PI, such as batch modification, copy and downloading;
c) The PI Controllers shall assign the roles of security administrators, data operators and auditors to different people;
d) Where the job requires to authorize a particular person to process the PI beyond his/her access, it shall be approved by the person or the department responsible for PI protection, and it shall be documented;

   Note 1: See 11.1 for the designation of the person or the department responsible for PI protection.

e) For such operations as access to and modification of sensitive PI, on top of a role-based access control mechanism, the PI Controllers should set the particular need arising in the business process as a trigger for certain operation authorization. For example, only after receiving a customer complaint may a complaint-handler access relevant information of such PI Subject.

7.2 Restrictions on display

Where display of PI on an interface (such as display screen and paper) is involved, the PI Controller should take measures such as de-identification to process the to-be-displayed PI, so as to reduce the risk of PI leakage during the display. For example, during the display of PI, the PI Controller could prevent unauthorized accesses to the PI by unauthorized internal personnel or by people other than the PI Subject.

7.3 Restrictions on the purpose of use

Requirements on PI Controllers include:

a) The use of PI shall not go beyond the scope directly or reasonably related to the purposes declared for the collection of PI. When business needs require the use of PI that exceeds the abovementioned scope, the PI Controller shall again seek explicit consent from PI Subjects.

   Note 1: Using the collected PI for academic research or making descriptions about the overall state of nature, science, society and economy is within the scope reasonably related to the collection purpose. However, when the academic research or description results are made available, the PI contained in the results shall be de-identified.

b) The information generated from the processing of collected PI, if able to, either independently or in combination with other information, identify a particular natural person or reflect the activity of a particular natural person, shall be deemed PI. Processing of such information shall fall within the scope of consent obtained for the collection of PI.

   Note 2: If the PI generated from the processing falls within the category of sensitive PI, processing of such information shall meet the requirements pertaining to sensitive PI.

7.4 Restrictions on the use of user profiling

Requirements on PI Controllers include:

a) In user profiling, the characteristic description of PI Subjects shall not:
   1) Contain obscene, pornographic, gamble-related, superstitious, horrific or violent contents;
   2) Contain contents that discriminate against nations, ethnic groups, religions, disabilities and diseases.

b) The use of user profiling in business operations or external business cooperation shall not:
   1) Infringe on the legitimate rights and interests of citizens, legal persons or other organizations;
   2) Jeopardize national security, national honor or interests, instigate the subversion of state power or the overturn of the socialist system, incite secession of the country or sabotage of national unity, advocate terrorism or extremism, propagate ethnic hatred or ethnic discrimination, spread violent, obscene or pornographic information, or fabricate or spread false information to disrupt the economic and social order.

c) Unless necessary to achieving the purpose of use of PI consented to by PI Subjects, in the use of PI, the explicit information that could point to the identity of a particular individual shall be removed. For example, direct user profiling could be used for the purpose of accurately evaluating the credit status of an individual, but for the purpose of pushing commercial advertisements, indirect user profiling should be used.

7.5 Use of personalized display

Requirements on PI Controllers include:

a) Where personalized display is used in the process of providing business functions to PI Subjects, the content of personalized display and the content of non-personalized display shall be distinguished significantly;

Note 1: Significant distinction includes but is not limited to: mark words such as "push", and display in different columns, sections, or on different pages.

b) Where personalized display that provides search results of goods or services based on customers’ interests, preferences, consumption habits, etc.is adopted in the process of providing e-commerce services to PI Subjects, the Controller shall also provide consumers with the options that do not target their personal characteristics;

Note 2：Displaying and ranking search results based on the specific geographical location that a PI Subject chooses without differentiating the content and search result ranking for different PI Subjects, falls within the category of options that do not target the personal characteristics of PI Subjects.

c) Where personalized display is used in the process of pushing news information services to PI Subjects, the PI Controller shall:

1) Provide a simple and intuitive option for the PI Subjects to exit or turn off the personalized display mode;

2) When a PI Subject exits or turns off the personalized display mode, provide the PI Subject with options to delete or anonymize the PI on which the targeted push activity is based.

d) Where personalized display is used in the process of providing business functions to PI Subjects, the PI Controller should establish a mechanisms for the PI Subjects to independently control the PI on which the personalized display depends (such as labels and profiling dimensions), to ensure the ability of the PI Subjects to adjust and control the degree of relevance of personalized display.

7.6 Fusion of PI collected for different business purposes

Requirements on PI Controllers include:

a) The PI Controllers shall comply with the requirements set in 7.3 of this document;

b) The PI Controllers shall carry out a PI security impact assessment and take effective PI protection measures in accordance with the purposes for which fusion of PI is to be used.

7.7 Use of automatic decision-making mechanism of information systems

For the information systems used in business operations of a PI Controller, which has an automatic decision-making mechanism and can have a significant impact on the legitimate rights and interests of PI Subjects (e.g. automatically determining personal credit and loan amount, or being used for automated screening of candidates), the PI Controller shall:

a) Conduct a PI security impact assessment during the planning and design phase or before the first use, and take effective measures to protect the PI Subjects in accordance with the result of the assessment;

b) Conduct security impact assessments on a regular basis (at least once a year) in the course of operation, and improve the measures that protect the PI Subjects in accordance with the results of the assessments;

c) Provide the PI Subjects with a channel of complaint against the results of automatic decision-making, and enable manual review on the results of automatic decision-making.

8 Rights of PI Subjects

8.1 Access

A PI Controller shall provide a PI Subject with access to the following information:

a) the PI or types of the PI of the Subject held by the PI Controller;

b) the source of the above-mentioned PI, as well as the purpose for which it is used;

c) the identity or type of any third party who has obtained the above-mentioned PI.

Note 1: When a PI Subject files an access request for the PI that was not provided voluntarily by the PI Subject, the PI Controller may take into account, among other factors, the potential risks and damages to the legitimate rights and interests of the PI Subject should it not respond to such request, as well as the technical feasibility and the cost of meeting the request, and then make a decision on whether to respond, and provide explanations.

8.2 Rectification

Where a PI Subject finds his/her PI held by a PI Controller erroneous or incomplete, the PI Controller shall provide a channel for the PI Subject to request to rectify the error or provide supplemental information.

8.3 Deletion

Requirements on PI Controllers include:

a) In the following cases, the PI in question shall be deleted without delay upon request for deletion from a PI Subject:

1) The PI Controller has collected and used PI in violation of laws or regulations;

2) The PI Controller has collected and used PI in violation of its agreement with the PI Subject.

b) If a PI Controller has shared PI with, or transferred PI to a third party in violation of laws or regulations, or in violation of its agreement with the PI Subject, and the PI Subject requests deletion, the PI Controller shall immediately stop the sharing and transfer, and notify the third party to delete the information in a timely manner.

c) If a PI Controller has publicly disclosed PI in violation of laws or regulations, or in violation of its agreement with the PI Subject, and the PI Subject requests deletion, the PI Controller shall immediately cease the disclosure and issue a notice requiring the recipients to delete the information.

8.4 Withdrawal of consent

Requirements on PI Controllers include:

a) The PI Controllers shall provide a method for PI Subjects to withdraw their consent to the collection and use of their PI; after the withdrawal of consent, the PI Controllers shall not continue to process relevant PI;

b) The PI Controllers shall ensure that PI Subjects have the right to refuse to receive the commercial advertisements pushed to them based on their PI; the PI Controllers shall also provide with the PI Subjects with a method to withdraw consent in the case of sharing, transferring or publicly disclosing PI.

Note 1: Withdrawal of consent does not affect the consent-based PI processing prior to the withdrawal.

8.5 De-registration

Requirements on PI Controllers include:

a) A PI Controller that provides products or services through registered accounts shall provide the method for de-registration to PI Subjects, and such method shall be easy to operate;

b) After a request for de-registration is accepted, if manual handling is required, verification and handling shall be completed within the promised time limit (not more than 15 working days);

c) If identity verification is needed during the process of de-registration, the types of PI to be re-provided by the PI Subject shall not be more than those collected during the service procedure such as registration and use;

d) The de-registration process shall not impose unreasonable conditions or make additional requirements to increase the obligation of the PI Subject, such as stipulating that the de-registration of a single account is deemed de-registration from multiple products or services, or requiring the PI Subject to provide accurate operating records as a necessary condition for the cancellation;

Note 1: If there is an essential link business-wise between multiple products or services, for example, the de-registration of an account for a product or service will result in the inability to implement necessary business functions of other products or services or a significant decline in the quality of service, a detailed statement of such circumstances shall be provided to the PI Subject.

Note 2: If a product or service does not have an independent account system, de-registration could be implemented by deleting the PI other than the product or service account, and cutting off the link between the account system and the product or service.

e) When sensitive PI is required to be collected for identity verification during the process of de-registration, measures for processing such information shall be clarified, such as deleting or anonymizing the information immediately after the purpose is achieved;

f) After a PI Subject de-registers, his/her PI shall be deleted or anonymized timely. If it is necessary to retain the PI due to laws and regulations, the information shall not be used again in daily business activities.

8.6 Obtaining a copy of PI

According to the request of a PI Subject, the PI Controller should provide the PI Subject with a method to obtain a copy of the following PI, or where technically feasible, transmit a copy of the following PI to the third party designated by the PI Subject:

a) Basic PI and identity information;

b) Personal health and physiological information, educational and occupational information.

8.7 Response to requests from PI Subjects

Requirements on PI Controllers include:

a) After verifying the identity of a PI Subject, the PI Controller shall make a timely response to the request of the PI Subject in accordance with 8.1-8.6, give a reply and reasonable explanation within 30 days or the time limit stipulated by laws or regulations, and inform the Subject of the method for external dispute settlement.

b) If a product or service is provided through an interactive interface (e.g. website, mobile-Internet application (APP), and client software), the PI Controller should set up a convenient interactive page to provide functions or options, so that PI Subjects could exercise online their rights such as access to and rectification & deletion of PI, consent withdrawal and de-registration.

c) In principle, no fee shall be charged for reasonable requests. For repeated requests over a period of time, a fee may be charged as appropriate.

d) If direct implementation of a PI Subject’s request involves high costs or significant difficulties, the PI Controller shall provide an alternative means to the PI Subject to protect the legitimate rights and interests of the PI Subject.

e) In the following cases, it is allowed not to respond to the request made by PI Subjects based on 8.1-8.6:

    1) In connection with the fulfilment of obligations under laws and regulations by the PI Controller;

    2) Directly related to national security or national defense;

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

    4) Directly related to criminal investigations, prosecutions, trials or execution of court decisions;

5) Where the PI Controller has ample evidence to show that a PI Subject has malicious intent or abuses his/her rights;

6) For the purpose of protecting the life, property or other significant legal rights and interests of a PI Subject or other individuals, and it is difficult to obtain consent from the PI Subject;

7) Where responding to a PI Subject’s request will bring about grave harm to the legitimate rights and interests of the PI Subject, other individuals or organizations;

8) Where trade secrets are involved.

f) If the decision is *Not to respond* to the request of a PI Subject, the PI Controller shall inform the PI Subject of the reasons on which this decision is based and provide the PI Subject with a channel for complaint.

8.8 Complaint management

PI Controllers shall establish a complaint management mechanism and a compliant tracking process, and respond to complaints within a reasonable time.

9 Entrusted processing, sharing, transfer and public disclosure of PI

9.1 Entrusted processing

When a Controller entrusts a third party to process PI, the following requirements shall be met:

a) The entrustment made by the PI Controller shall not go beyond the scope of the consent of PI Subjects or shall fall within the circumstances listed in 5.6;

b) The PI Controller shall conduct a PI security impact assessment for the entrustment, and ensure that the trustee meets the data security capacity requirements set in 11.5;

c) The trustee shall:

1) Process the PI in strict accordance with the requirements of the PI Controller; if the trustee fails to do so due to a special reason, it shall notify the PI Controller promptly;

2) Obtain prior authorization from the PI Controller if the trustee needs to sub-entrust;

3) Assist the PI Controller to respond to requests made by PI Subjects based on 8.1-8.6;

4) Promptly notify the PI Controller if the trustee is unable to provide adequate level of security or in case of a security incident in the process of PI processing;

5) Not store relevant PI anymore upon termination of the entrustment.

d) The PI Controller shall supervise the trustee through methods including but not limited to:

1) Specify the responsibilities and obligations of the trustee through contracts or otherwise;

2) Audit the trustee.

e) The PI Controller shall accurately record and store the entrusted PI processing.

f) If the PI Controller learns or discovers that the trustee has failed to process the PI in accordance with the entrustment requirements, or failed to effectively fulfill the responsibility for PI protection, the PI Controller shall immediately require the trustee to stop relevant activities and shall take or require the trustee to take effective remedial measures (such as changing the password, revoking access, and disconnecting the network) to control or eliminate the security risks to the PI. If necessary, the PI Controller shall terminate its business relationship with the trustee and require the trustee to delete the PI obtained from the PI Controller in time.

9.2 Sharing and transfer

When sharing and transferring PI, PI Controllers shall pay full attention to risks. If PI is shared and transferred not due to acquisition, merger, reorganization or bankruptcy, the following requirements shall be met:

a) A security impact assessment of PI shall be conducted in advance, and effective measures to protect PI Subjects shall be taken based on the assessment results.

b) The PI Subjects shall be informed of the purpose of the sharing and transfer, the type of the data recipient and possible consequences, and consent of the PI Subjects shall be obtained in advance. Cases are excepted where the PI to be shared is de-identified and it is ensured that the data recipient cannot re-identify or associate the PI Subjects;

c) Before sharing or transferring sensitive PI, in addition to the information set in 9.2 b) that is to be provided to the PI Subjects, the PI Controllers shall also inform the PI Subjects of the types of sensitive PI involved, the identity of the recipient and their data security capabilities, and obtain explicit consent of the PI Subjects in advance;

d) The PI Controllers shall specify the responsibilities and obligations of the data recipient through contracts or otherwise;

e) The PI Controllers shall accurately record and store information about PI sharing and transfer, including the date, scale, purpose of the sharing and transfer, and basic information of the data recipient;

f) If a Controller discovers that the data recipient has processed the PI in violation of the requirements of laws or regulations or the agreement between the two parties, the PI Controller shall immediately require the data recipient to stop relevant activities and shall take or require the data recipient to take effective remedial measures (such as changing the password, revoking access, and disconnecting the network) to control or eliminate the security risks to the PI; if necessary, the PI Controller shall terminate its business relationship with the data recipient, and require the data recipient to delete the PI obtained from the PI Controller in time;

g) The PI Controllers shall bear the corresponding responsibility for any damage on the legitimate rights and interests of the PI Subjects incurred by security incidents due to the sharing and transfer of PI;

h) The PI Controllers shall help the PI Subjects to understand the storage and use of PI by data recipients, as well as the rights of the PI Subjects, such as the right to access, rectify, delete information and to de-register;

i) Personal biometric information shall not, in principle, be shared or transferred. If it is necessary to share or transfer due to business needs, the PI Controller shall inform each PI Subject of the purpose, the types of personal biometric information involved, the specific identity and data security capabilities of the data recipient, etc., and obtain explicit consent from the PI Subjects.

9.3 Transfer of PI in the case of acquisition, merger, reorganization or bankruptcy

If a PI Controller undergoes a merger, acquisition, reorganization, bankruptcy or other kinds of change, the following requirements shall be met:

a) The PI Subjects shall be informed of the situation;

b) The new PI Controller shall continue to fulfill the responsibilities and obligations of the original PI Controller. If the use purpose of PI is changed, the PI Controller shall re-seek explicit consent the PI Subjects;

c) In the case of a bankruptcy with no undertaker, data shall be deleted.

9.4 Public disclosure

PI shall, in principle, not be publicly disclosed. When a PI Controller is authorized by law or has reasonable causes for public disclosure, the following requirements shall be met:

a) The PI Controller shall conduct a PI security impact assessment in advance, and take effective measures based on the assessment results to protect PI Subjects;

b) The PI Controller shall notify the PI Subjects of the purpose of the public disclosure and the types of PI to be publicly disclosed, and shall obtain explicit consent from the PI Subjects prior to the disclosure;

c) Before the public disclosure of sensitive PI, in addition to the information set in 9.4 b), the PI Subjects shall also be informed of the content of the sensitive PI involved in the public disclosure;

d) The public disclosure of PI shall be accurately recorded and stored, including the date, scale, purpose and scope of such disclosure;

e) The PI Controller shall bear the corresponding responsibility for any damage to the legitimate rights and interests of the PI Subjects due to the public disclosure of PI;

f) Personal biometric information shall not, in principle, be publicly disclosed;

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

9.5 Exceptions to obtaining consent prior to the sharing, transfer or public disclosure of PI

In the following cases, the sharing, transfer and public disclosure of PI by the PI Controller does not require prior consent of PI Subjects:

a) In connection with the fulfilment of obligations under laws and regulations by the PI Controller;

b) Directly related to national security or national defense;

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

d) Directly related to criminal investigations, prosecutions, trials or execution of court decisions;

e) For the purpose of safeguarding the life, property or other significant lawful rights and interests of a PI Subject or other individuals, and it is hard to obtain consent from the PI Subject;

f) The PI is proactively disclosed to the public by the PI Subject;

g) The PI is collected from legally and publicly disclosed information, such as legal news reports and government information disclosure.

9.6 Common controllers of PI

Requirements on PI Controller include:

a) If a PI Controller and a third party are common controllers of PI, the PI Controller shall, through contracts or other means, jointly determine with the third party the PI security requirements to be met, clarify their respective responsibilities and obligations, and inform PI Subjects clearly;

b) If a PI Controller fails to explicitly inform the PI Subjects of the identity of the third party and the PI security responsibilities and obligations borne by the PI Controller and the third party respectively, the PI Controller shall bear the responsibility for any PI security incident caused by the third party.

   Note 1: If the PI Controller deployed a third-party plugin to collect PI during the delivery of a product or service (for example, a website operator deploys statistical analysis tools, software development kits (SDKs), or map APIs on its web pages or in its applications) and the third-party did not separately obtain consent from the PI Subjects for collecting their PI, then the PI Controller and the third party are common controllers of PI during the PI collection period.

9.7 Third-party access management

If a PI Controller introduces into its products or services a third-party product or service that has the function of collecting PI, and if 9.1 and 9.6 do not apply, the requirements on the PI Controller include:

a) The PI Controller shall establish a management mechanism and working process for the introduction of third-party products or services, and set mechanisms such as a security assessment as the condition for the introduction when necessary;

b) The PI Controller shall specify the security responsibilities of and the PI security measures to be implemented by both parties by way of a contract with the third-party product or service provider or other means;

c) The PI Controller shall explicitly mark the product or service provided by the third party to inform PI Subjects;

d) The PI Controller shall properly retain contracts and management records related to third-party access to the platform and ensure these records are available to relevant parties;

e) The PI Controller shall require the third party to obtain consent from the PI Subjects for collecting PI in accordance relevant requirements of this document and if necessary, verify the realization method;

f) The PI Controller shall require the third-party product or service provider to establish mechanisms to respond to the PI Subjects' requests, complaints, etc., so that the PI Subjects can access and use;

g) The PI Controller shall supervise the third-party product or service provider to strengthen the security management of PI, promptly urge rectification once it discovers the provider did not fulfill security management requirements and responsibilities, and revoke its access if necessary;

h) In the case where a product or service is embedded with or connected to a third-party automation tool (such as code, script, interface, algorithm model, software development kit, and mini program), the following measures should be taken:

  1) Conduct technical testing to ensure that the collection and use of PI meets the agreed requirements;

  2) Audit the collection of PI by the automation tool embedded or connected by the third party and cut off its access in time upon discovery of any behavior beyond the agreed scope.

9.8 Cross-border transfer

Where the PI collected and generated during operations within the territory of the People's Republic of China is provided overseas, the PI Controller shall conform to the requirements of relevant national regulations and standards.

10 Handling of PI security incidents

10.1 Emergency handling and reporting of PI security incidents

Requirements on PI Controllers include:

a) The PI Controllers shall develop an emergency response plan for PI security incidents;

b) The PI Controllers shall organize emergency response trainings and emergency drills on a regular basis (at least once a year) for relevant personnel, to enable them to understand their duties as well as emergency response policies and procedures;

c) After a PI security incident occurs, the PI Controller shall carry out the following actions based on the emergency response plan:

1) Record the details of about the incident, including but not limited to: the person who discovered the incident, the time and location of the incident, the PI and number of PI Subjects involved, the name of the system involved, the impacts on other connected systems, and whether the law enforcement agency or a relevant department has been contacted;

2) Assess possible impacts of the incident, and take necessary measures to control the situation and eliminate underlying risks;

3) Make a timely reporting in accordance with the National Emergency Plan for Cyber Security Incidents and other relevant regulations, the content of which shall include but not be limited to: general information about the incident, such as the type and number of the PI Subjects involved, the details and nature of the incident, possible impacts of the incident, handling measures that have been taken and will be taken, and contact information of the persons handling the incident;

4) In the case where the PI leakage may seriously jeopardize the legal rights and interests of PI Subjects, such as a leakage of sensitive PI, a notification of the security incident shall be made in accordance with the requirements set in 10.2.

d) The PI Controllers shall update the emergency plan in a timely manner to reflect changes in relevant laws and regulations, and based on the handling of incidents.

10.2 Notification of PI security incidents

Requirements on PI Controllers include:

a) The PI Controllers shall notify the PI Subjects affected in time through email, correspondence, telephone, push notification or other means. Where it is difficult to notify the PI Subjects one by one, a public alert shall be released in a reasonable and effective manner;

b) The notification shall include but not be limited to:

1) Details about the security incident and its impacts;

2) Handling measures that have been taken and will be taken;

3) Recommendations for the PI Subjects to prevent and reduce risks on their own;

4) Remedial measures provided to the PI Subjects;

5) Contact information of the person and department responsible for PI protection.

11 PI security management requirements for organizations

11.1 Specifying responsible department and person

Requirements on PI Controllers include:

a) The PI Controllers shall clearly state that the legal representative or the principal shall take overall responsibility for PI security, including providing human resources, financial resources and material resources for PI security work;

b) The PI Controllers shall appoint a person and a department responsible for PI protection. The person responsible for PI protection shall be someone who has relevant management experience and PI protection expertise, who shall participate in important decisions on PI processing activities and report directly to the principal of the organization;

c) An organization that meets any of the following conditions shall set up a full-time post and a department dedicated to PI security work:

   1) Main business involves the processing of PI, and the number of employees exceeds 200;
   2) Processes the PI of more than 1,000,000 individuals, or is estimated to process the PI of more than 1,000,000 individuals;
   3) Processes the sensitive PI of more than 100,000 individuals.

d) The responsibilities of the person and the department responsible for PI protection shall include, but not be limited to:

   1) Coordinate the internal PI security efforts of the organization, and bear direct responsibility for PI security;
   2) Organize the development of a PI protection work plan and supervise and urge the implementation;
   3) Draft, issue, implement and regularly update PI protection policies and related procedures;
   4) Establish, maintain and update a list of the PI the organization possesses (including the type, amount, source and the recipient of the PI) and the policy for access authorization;
   5) Carry out PI security impact assessments, put forward measures and suggestions for PI protection and supervise and urge the rectification of security risks;
   6) Organize PI security trainings;
   7) Conduct testing before the release of products or services to avoid the unknown PI collection, use, sharing and other processing activities;
   8) Publish information such as the channel for complaints and tip-offs, and accept and handle the complaints and tip-offs in time;
   9) Conduct security audits;
   10) Liaise with the supervision and management departments to inform them of or report to them the status of PI protection and incident handling.

e) The PI Controllers shall provide necessary resources to the person and the department responsible for PI protection to ensure the independent performance of their duties.

11.2 PI security engineering

When developing a product or service that has the function of processing PI, the PI Controller should, in accordance with relevant national standards, take PI protection requirements into consideration in the system engineering phases of demand analysis, design, development, testing, release, etc., and ensure that PI protection measures are planned, deployed and used in sync with the system development.

11.3 Records of PI processing activities

PI Controllers shall establish, maintain and update the records of processing activities of the PI collected and used, the content of which may include:

a) The type, amount and source (for example, directly collected from PI Subjects or acquired indirectly) of the PI involved;

b) Differentiated processing purposes and use scenarios of PI based on business functions and consent, as well as information such as entrusted processing, sharing, transfer, public disclosure and whether cross-border transfer is involved;

c) Information systems, organizations and personnel associated with every step of the PI processing activity.

11.4 PI security impact assessment

Requirements on PI Controllers include:

a) The PI Controllers shall establish a PI security impact assessment system to assess and address security risks associated with PI processing activities;

b) The PI security impact assessment shall mainly assess the compliance of processing activities with the basic principles of PI security, and the impacts of PI processing activities on the lawful rights and interests of PI Subjects, including but not limited to:

   1) Whether the collection of PI complies with the principles of explicit purposes, independent consent and minimum necessary;

   2) Whether the processing of PI may cause adverse impacts on the lawful rights and interests of PI Subjects, including whether it could endanger personal or property safety, damage personal reputation or physical & mental health, or lead to differentiated treatment;

   3) The effectiveness of PI security measures;

   4) Risks that the anonymized or de-identified data set, either alone or converged with other data sets, becomes identifying again;

   5) Possible adverse impacts of the sharing, transfer and public disclosure of PI on the lawful rights and interests of PI Subjects;

   6) Possible adverse impacts on the lawful rights and interests of PI Subjects in the case of a security incident;

c) The PI Controllers shall conduct a PI security impact assessment before the release of a product or service, or when a major change takes place in the business functions;

d) The PI Controllers shall conduct a PI security impact assessment when new legislative requirements come into effect, or when a major change occurs in business models, information systems, or operation environments, or when a significant PI security incident occurs;

e) A PI security assessment report shall be formed, based on which the PI Controller shall adopt measures to protect PI Subjects so as to reduce the risks to an acceptable level;

f) The PI security assessment report shall be properly retained, kept available to relevant parties, and made public in an appropriate form.

11.5 Data security capabilities

PI Controllers shall, based on the requirements of relevant national standards, develop appropriate data security capabilities and implement necessary management and technical measures to prevent the leakage, damage, loss and tampering of PI.

11.6 Personnel management and training

Requirements on PI Controllers include:

a) The PI Controllers shall sign a confidential agreement with relevant personnel on the posts involving PI processing, and conduct background checks on those who have extensive access to sensitive PI to understand their criminal records, integrity status, etc.;

b) The PI Controllers shall specify the security responsibilities of different posts involving PI processing, and establish penalty mechanisms for security incidents;

c) The PI Controllers shall explicitly require relevant personnel on the posts involving PI processing to continue to perform their confidentiality obligations when they are transferred out of the post or their employment contract terminates;

d) The PI Controllers shall clarify the PI security requirements for external service personnel who may have access to the PI, sign confidentiality agreements with them and conduct supervision;

e) The PI Controllers shall establish appropriate internal rules and policies to provide PI protection guidance and requirements for employees;

f) The PI Controllers shall organize professional trainings and examinations on PI security for relevant personnel on the posts involving PI processing on a regular basis (at least once a year) or when there is a major change to PI protection policies, so as to ensure that relevant personnel are proficient in PI protection policies and relevant procedures.

11.7 Security audit

Requirements on PI Controllers include:

a) The effectiveness of PI protection policies, relevant procedures and security measures shall be audited;

b) An automated audit system shall be established to monitor and record PI processing activities;

c) Records of the audit process shall be able to provide support for security incident handling, emergency response and post-event investigations;

d) Unauthorized access to, tampering with or deletion of audit records shall be prevented;

e) Illegal use and abuse of PI discovered during audits shall be handled in time;

f) Audit records and retention time shall follow the requirements of laws and regulations.

Annex A

(Informative)

Examples of personal information

PI refers to any information, recorded electronically or otherwise, that can be used alone or in combination with other information to identify a natural person or reflect the activities of a natural person, including but not limited to the name, date of birth, ID number, personal biometric information, residential address, contact information, communication records and content, user names and passwords, property information, credit information, records of whereabouts, accommodation information, health and physiological information, and transaction information.

To determine whether a particular piece of information is PI, the following two approaches shall be considered: First, information identifying individuals, that is, PI is the information that could help one identify a specific natural person through the specificity of the information; Second, information associated with individuals, that is, the information generated in the activities of a known natural person (such as the person’s location information, call logs and browsing history) is PI. Information that meets either of the two criteria above shall be determined as PI.

Table A.1 gives examples of PI.

Table A.1 Examples of personal information

Basic personal information	Name, date of birth, gender, ethnic group, nationality, family relation, address, personal phone number, email address, etc.
Personal identity information	ID card, military officer certificate, passport, driver’s license, employee ID, pass, social security card, resident certificate, etc.
Personal biometric information	Personal gene, fingerprint, voice print, palm print, auricle, iris, and facial recognition features, etc.
Online identity information	A PI subject’s account, IP address, and personal digital certificate.
Physiological and health information	Records generated in connection with medical treatment, such as pathological information, hospitalization records, physician’s instructions, test reports, surgical and anesthesia records, nursing records, medication administration records, drug and food allergy, fertility information, medical history, diagnosis and treatment, family illness history, history of present illness, and history of infection, and personal health information such as weight, height, and lung capacity.
Personal education information	Personal occupation, position, work unit, educational background, academic degree, educational experience, work experience, training records, transcript, etc.
Personal property information	Bank account, authentication information (password), bank deposit information (including amount of funds, payment and collection records), real estate information, credit records, credit information, transaction and consumption records, bank statement, etc., and virtual property information such as virtual currency, virtual transaction and game CD Keys.

Personal communication information	Communications records and content, SMS, MMS, emails, data that describe personal communications (often referred to as metadata), etc.
Contact information	Contacts, friend list, list of chat groups, email address list, etc.
Personal web surfing record	Refers to records of a PI Subject’s operations stored in the logs, including web browsing records, software use records, click records, and favorites.
Information of often used equipment	Refers to the information describing the general conditions of the equipment often used by an individual, including hardware serial number, equipment MAC address, list of software, and unique equipment identifier (e.g. IMEI/Android ID/IDFA/Open UDID/GUID, SIM card IMSI information).
Personal location information	Including records of whereabouts, precise location information, accommodation information, longitude and latitude.
Other information	Marriage history, religious preference, sexual orientation, undisclosed criminal records, etc.

Annex B
(Informative)

Identification of sensitive personal information

Sensitive PI refers to the information vital to personal interests, that once leaked, illegally provided, or misused, may endanger personal and property safety, or easily lead to damage to one’s personal reputation, mental & physical health, or discriminatory treatment. Generally, the PI of children up to 14 years of age and the information involving a natural persons’ privacy fall within the category of sensitive PI. The following aspects should be considered when determining whether a piece of information is sensitive PI:

Leakage: The leakage of PI will cause PI Subjects and the organizations collecting and using PI to lose control over the PI, leading to uncontrollability over the spreading and use of the PI. Some PI, once leaked, is used directly or analyzed in combination with other information against the will of the PI Subjects, which may bring major risks to the rights and interests of the PI Subjects. Such PI shall be determined as sensitive PI. For example, the photocopy of a PI Subject’s ID card is used by people other than the PI Subject for real-name registration for SIM cards and opening bank accounts.

Illegal provision: The information that, once spread beyond the scope of consent of the Subjects, will bring major risks to the rights and interests of the Subjects, shall be determined as sensitive PI. Such information includes sexual orientation, bank deposit information, and history of contagious diseases.

Misuse: The information that, once used beyond the limit of the consented scope (e.g. change of use purposes, expanded processing scope), may bring major risks to the rights and interests of the PI Subjects, shall be determined as sensitive PI. For example, insurance companies use personal health information for marketing purposes and to determine the premium level without prior consent of the PI Subjects.

Table B.1 gives examples of sensitive PI.

Table B.1 Examples of sensitive personal information

Personal property information	Bank account, authentication information (password), bank deposit information (including amount of funds, payment and collection records), real estate information, credit records, credit information, transaction and consumption records, bank statement, etc., and virtual property information such as virtual currency, virtual transaction and game CD Keys.
Physiological and health information	The records generated in connection with medical treatment, including pathological information, hospitalization records, physician’s instructions, test reports, surgical and anesthesia records, nursing records, medicine administration records, drug and food allergy, fertility information, medical history, diagnosis and treatment, family illness history, history of present illness, history of infection.
Personal biometric information	Personal gene, fingerprint, voice print, palm print, auricle, iris, and facial recognition features, etc.
Personal identity information	ID card, military officer certificate, passport, driver’s license, employee ID, social security card, resident certificate, etc.

Other information	Sexual orientation, marriage history, religious preference, undisclosed criminal records, communications records and content, contacts, friends list, list of chat groups, records of whereabouts, web browsing history, precise location information, accommodation information, etc.

Annex C
(Informative)

Methods to safeguard independent choice of personal information subject

C.1 Overview

Safeguarding the independent choice of PI Subjects includes two aspects: firstly, not force the PI Subjects to accept multiple business functions, and secondly, guarantee the PI Subjects' right to know about the collection and use of their PI and their right to give consent. PI Controllers, especially operators of mobile-Internet applications (APPs), can do this through the following ways:

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

To ensure PI Subjects' independent right to choose and give consent, PI Controllers shall firstly draw a line between the basic business functions and extended business functions of a product or service. Methods are as follows:

a) The PI Controllers shall define the product or service's basic business functions in accordance with the fundamental expectations and the most important needs for the products or service that is selected or used by the PI Subjects;

   Note 1: A PI Subject identifies or selects a product or service based primarily on such factors as the marketing and business positioning of the product or service provided by the PI Controller, the name of the product or service itself, the description in the app store, and the category of application. Therefore, the PI Controller shall define the basic business functions based on the average PI Subjects' most likely knowledge and understanding of the above factors, rather than their own ideas to determine the PI Subjects' main needs and expectations. In general, basic business functions are those that if not provided, the PI Subjects would not choose to use the product or service.

   Note 2: As products or services iterate, expand and upgrade, their basic business functions may need to be redefined. PI Controllers may still redefine the basic business functions based on the most likely knowledge and understanding of average PI Subjects. However, the PI Controllers should not change the demarcation between basic business functions and extended business functions on a large scale in a short period of time. After redefinition, the PI Controllers should again inform the PI Subjects and obtain their explicit consent regarding the collection and use of their PI for basic business functions;

b) Improving service quality, enhancing PI Subjects' experience, or the R&D of new products shall not be deemed a separate basic business function;

c) All the functions provided by the product or service other than the basic business functions shall be defined as extended business functions.

C.3 Notification of basic business functions and explicit consent

Methods to deliver basic business function notification and obtain explicit consent are as follows:

a) PI Controllers shall, before the basic business functions are activated (such as the initial installation, first use, and account registration by PI Subjects), inform the PI Subjects of the types of PI necessary to be collected for basic business functions through an interactive interface or design (such as pop-up windows, text descriptions, filling boxes, tooltips, and warning tones), as well as the impact resulted if the PI Subject refuses to provide or refuses to consent to the collection, and take the affirmative action of the PI Subjects (such as tick or click "Agree" or "Next") as explicit consent to the collection；

   Note 1: When the basic business functions provided by a product or service do not need to be activated all at once, they should be gradually activated in accordance with the specific use behavior of the PI Subject, and the notification requirements in a) should be completed immediately.

b) When a PI Subject rejects the collection of PI necessary for basic business functions, the PI Controller may refuse to provide the business functions to the PI Subject；

c) The interactive interface or design required in C.3 a) shall make it convenient for PI Subjects to re-access and change the scope of the consent.

   Note 2: See Annex C.5 for the implementation of the requirements above.

C.4 Notification of extended business functions and explicit consent

Methods to deliver extended business function notification and obtain explicit consent are as follows:

a) PI Controllers shall, before extended business functions are used for the first time, inform individual PI Subjects of the extended business functions and the types of PI necessary to be collected, through an interactive interface or design (such as pop-up windows, text descriptions, filling boxes, tooltips and warning tones), and allow the PI Subjects to opt in for each extended business function；

b) If a PI Subject rejects the collection of the PI necessary for extended business functions, the PI Controller shall not repeatedly ask the PI Subject for consent. Unless the PI Subject proactively chooses to activate an extended business function, the number of requests for consent to the PI Subject shall not exceed once in 48 hours;

c) If a PI Subject rejects the collection of the PI necessary for extended business functions, the PI Controller shall not refuse to provide basic business functions or reduce the quality of service of basic business functions;

d) The interactive interface or design required in C.4 a) shall make it convenient for PI Subjects to re-access and change the scope of consent.

   Note 1: See Annex C.5 for the implementation of the requirements above.

C.5 Design of interactive interface

PI Controllers may design an interactive interface by reference to Table C.1 so as to protect PI Subjects' full exercise of their right to choose and to give consent.

Such an interface shall be proactively provided by the PI Controller to the PI Subjects before the PI Controller commences the collection of PI, in the course of product installation, when a PI Subject uses a product or service for the first time, and when the a PI Subject creates an account. In the event where sensitive PI is collected via written materials, the PI Controller may design the interface by reference to the following template so as to protect the PI Subjects' full exercise of their right to choose and to give consent.

Table C.1 Template of interactive interface

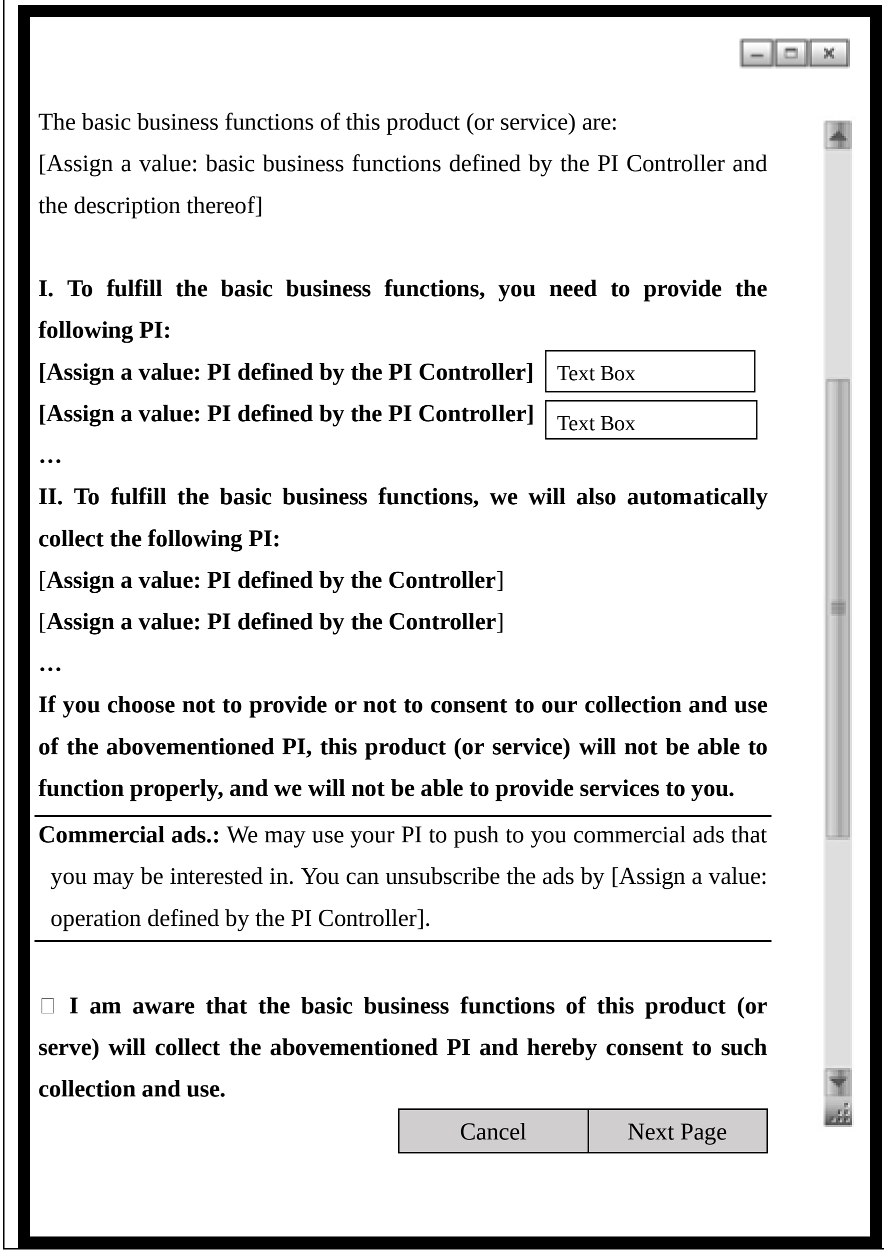
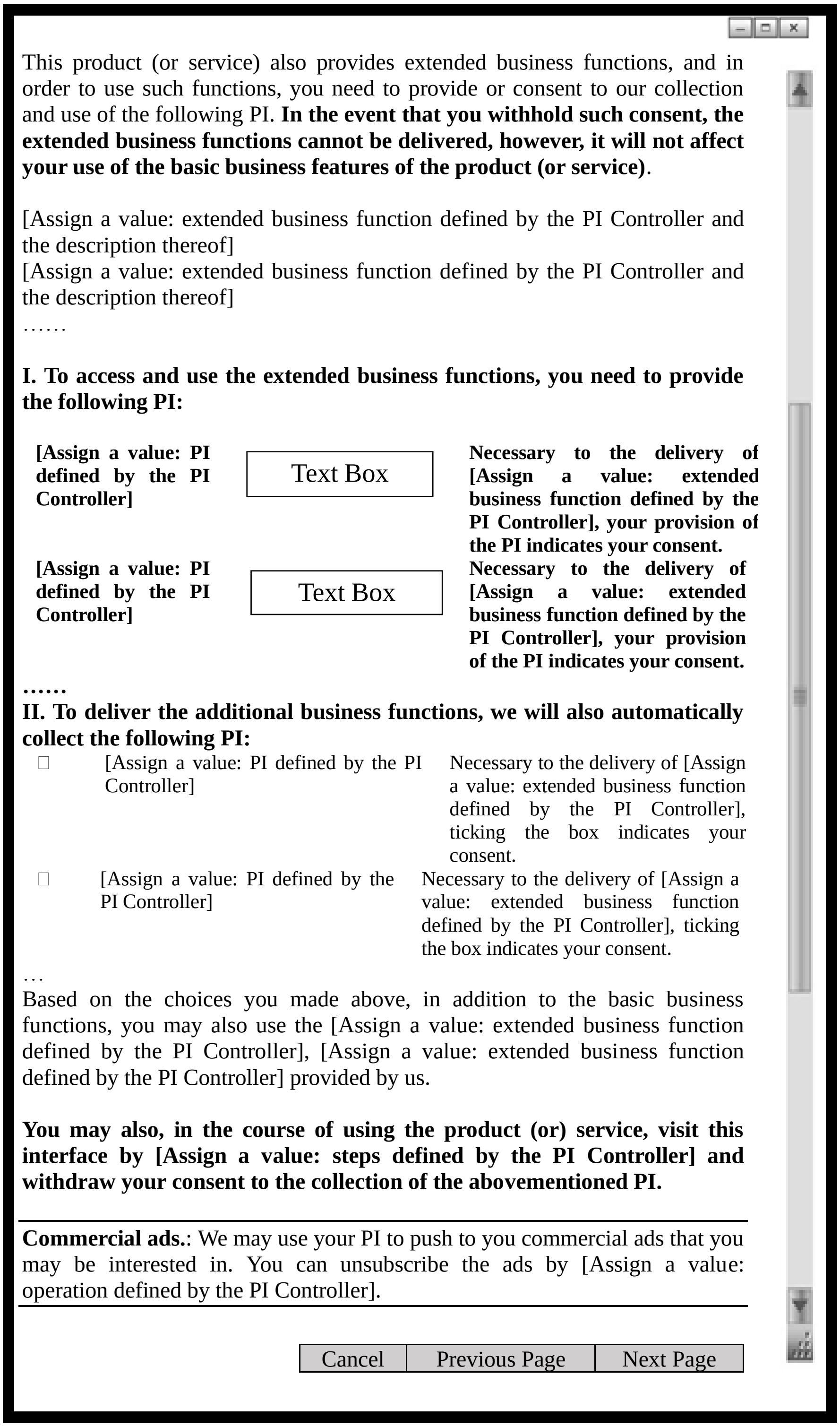
Interface Template	**Explanation**
Interface 1: PI Collection for Basic Business Functions  The basic business functions of this product (or service) are: [Assign a value: basic business functions defined by the PI Controller and the description thereof] **I. To fulfill the basic business functions, you need to provide the following PI:** **[Assign a value: PI defined by the PI Controller]** Text Box **[Assign a value: PI defined by the PI Controller]** Text Box … **II. To fulfill the basic business functions, we will also automatically collect the following PI:** [**Assign a value: PI defined by the Controller**] [**Assign a value: PI defined by the Controller**] … **If you choose not to provide or not to consent to our collection and use of the abovementioned PI, this product (or service) will not be able to function properly, and we will not be able to provide services to you.** **Commercial ads.:** We may use your PI to push to you commercial ads that you may be interested in. You can unsubscribe the ads by [Assign a value: operation defined by the PI Controller]. □ **I am aware that the basic business functions of this product (or serve) will collect the abovementioned PI and hereby consent to such collection and use.** Cancel Next Page	1. In order to clearly show the purpose, types, etc. of the PI collection to PI Subjects, and to obtain their consent on a case by case basis, we suggest that PI Controllers display the content shown in the template on the left to the PI Subjects on different phases, in different windows and on different screens. 2. The PI Controller shall explicitly define the basic business functions of its product (or service) and identify the PI that needs to be collected. 3. Where the assignment of value is needed in the template on the left, the PI Controller shall fill it in according to the actual situation, and the content thereof shall be clear and understandable. In addition, no general or ambiguous wording shall be used to describe the PI to be collected. 4. When delivering the features in the template on the left, the PI Controllers may take into consideration the actual form of the product (or service) as well as the factor of appropriateness and convenience. 5. When delivering the features in the template on the left, the tick box shall not be ticked on default.

Table C.1 (continued)

Interface 2: PI Collection for Extended Business Functions



This product (or service) also provides extended business functions, and in order to use such functions, you need to provide or consent to our collection and use of the following PI. **In the event that you withhold such consent, the extended business functions cannot be delivered, however, it will not affect your use of the basic business features of the product (or service)**.

[Assign a value: extended business function defined by the PI Controller and the description thereof]
[Assign a value: extended business function defined by the PI Controller and the description thereof]
……

I. To access and use the extended business functions, you need to provide the following PI:

[Assign a value: PI defined by the PI Controller]	Text Box	**Necessary to the delivery of [Assign a value: extended business function defined by the PI Controller], your provision of the PI indicates your consent.**
[Assign a value: PI defined by the PI Controller]	Text Box	**Necessary to the delivery of [Assign a value: extended business function defined by the PI Controller], your provision of the PI indicates your consent.**

……

II. To deliver the additional business functions, we will also automatically collect the following PI:

□	[Assign a value: PI defined by the PI Controller]	Necessary to the delivery of [Assign a value: extended business function defined by the PI Controller], ticking the box indicates your consent.
□	[Assign a value: PI defined by the PI Controller]	Necessary to the delivery of [Assign a value: extended business function defined by the PI Controller], ticking the box indicates your consent.

…

Based on the choices you made above, in addition to the basic business functions, you may also use the [Assign a value: extended business function defined by the PI Controller], [Assign a value: extended business function defined by the PI Controller] provided by us.

You may also, in the course of using the product (or) service, visit this interface by [Assign a value: steps defined by the PI Controller] and withdraw your consent to the collection of the abovementioned PI.

Commercial ads.: We may use your PI to push to you commercial ads that you may be interested in. You can unsubscribe the ads by [Assign a value: operation defined by the PI Controller].

6. Extended business functions are the functions other than the basic business functions. Common extended business functions include: derivative functions or new-type functions on top of the basic business functions, add-on functions to improve the experience of using the product or service (such as voice recognition, image recognition and geographical location), and extended business functions to enhance the security mechanism of the product or service (such as collection of password-protected email address and fingerprints).

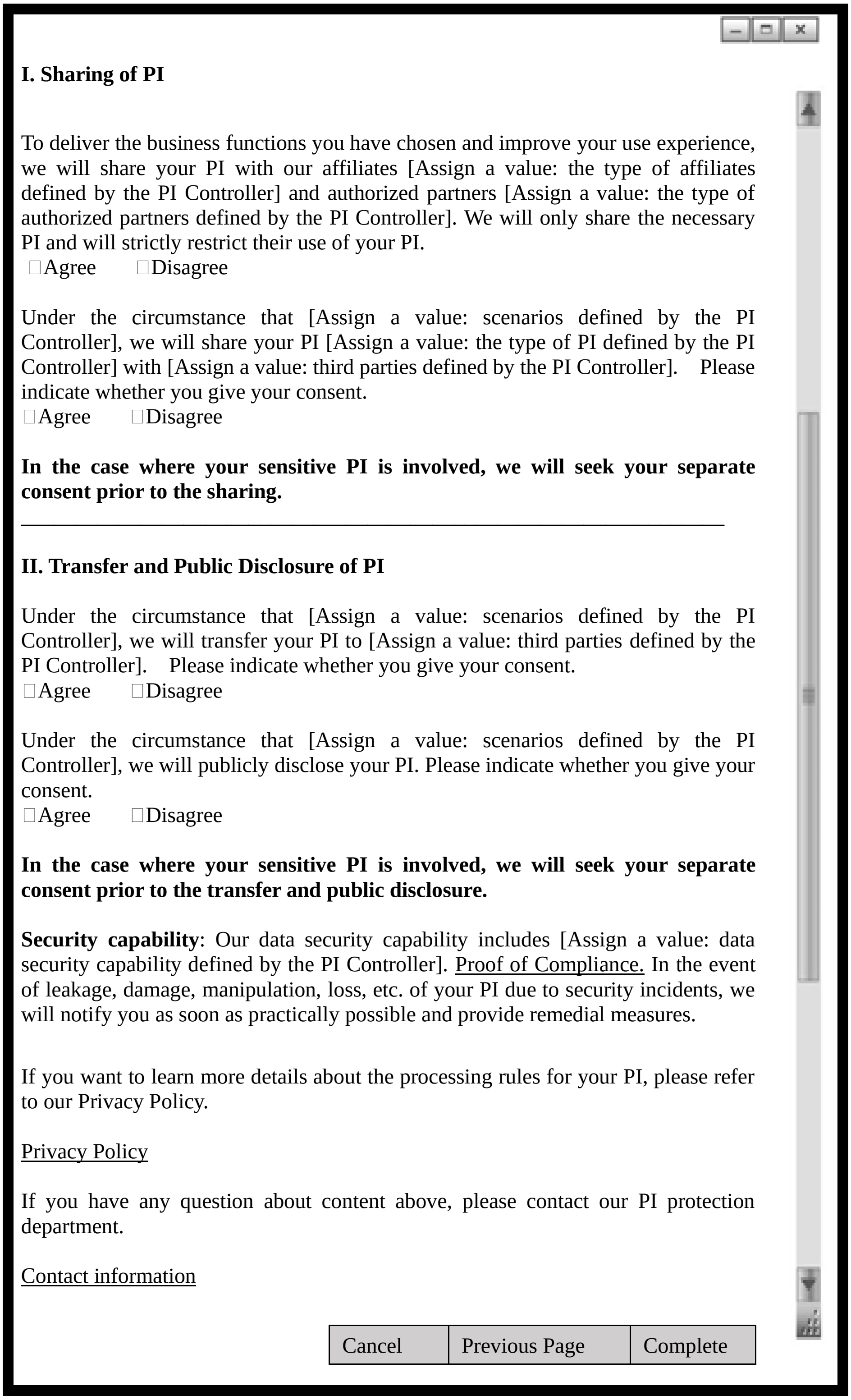
7. Generally, extended business functions are choice-based, can be unsubscribed and do not affect the basic business functions. PI Controllers shall fully analyze whether a business function has these features when determining extended business functions, and shall not treat extended business functions as basic business functions to forcibly collect PI.

8. On this page, PI Controllers may promptly display the extended functions available to the PI subject based on the PI voluntarily provided by the PI subject and the PI whose automatic collection the PI subject has consented to.

9. PI Controllers shall inform PI Subjects of how to visit this interface again in the future to protect the right of the PI subjects to withdraw their consent.

Table C.1 (continued)

Interface 3: Sharing, Transfer and Public Disclosure of PI



I. Sharing of PI

To deliver the business functions you have chosen and improve your use experience, we will share your PI with our affiliates [Assign a value: the type of affiliates defined by the PI Controller] and authorized partners [Assign a value: the type of authorized partners defined by the PI Controller]. We will only share the necessary PI and will strictly restrict their use of your PI.

□Agree □Disagree

Under the circumstance that [Assign a value: scenarios defined by the PI Controller], we will share your PI [Assign a value: the type of PI defined by the PI Controller] with [Assign a value: third parties defined by the PI Controller]. Please indicate whether you give your consent.

□Agree □Disagree

In the case where your sensitive PI is involved, we will seek your separate consent prior to the sharing.

II. Transfer and Public Disclosure of PI

Under the circumstance that [Assign a value: scenarios defined by the PI Controller], we will transfer your PI to [Assign a value: third parties defined by the PI Controller]. Please indicate whether you give your consent.

□Agree □Disagree

Under the circumstance that [Assign a value: scenarios defined by the PI Controller], we will publicly disclose your PI. Please indicate whether you give your consent.

□Agree □Disagree

In the case where your sensitive PI is involved, we will seek your separate consent prior to the transfer and public disclosure.

Security capability: Our data security capability includes [Assign a value: data security capability defined by the PI Controller]. Proof of Compliance. In the event of leakage, damage, manipulation, loss, etc. of your PI due to security incidents, we will notify you as soon as practically possible and provide remedial measures.

If you want to learn more details about the processing rules for your PI, please refer to our Privacy Policy.

Privacy Policy

If you have any question about content above, please contact our PI protection department.

Contact information

10. The circumstances under which the PI may be shared with, transferred to a third party or publicly disclosed may diversify due to complicated business functions. PI Controllers may, as appropriate, add to the page the scenarios of sharing, transfer, or public disclosure of data, or inform PI Subjects via a pop-up window or other means, and seek their consent during their process of use.

11. Data security capability refers to the capability of a PI Controller to protect the confidentiality, integrity and availability of PI. A PI Controller may demonstrate its data security capability by carrying out national standards compliance tests, and display the proof to PI Subjects via links attached.

12. PI Controllers shall provide PI Subjects with access to Q&As regarding the processing rules, and if a PI Subject does not accept such processing rules, the PI Subject may choose to discontinue the use of such product or service.

13. PI Subjects shall be provided with means to contact the PI Controller.

14. PI Controllers shall provide a link to the PI protection policy for the reference of PI Subjects.

Annex D
(Informative)

Personal information protection policy template

A published PI protection policy is an important manifestation of the PI Controller following the principle of openness and transparency, an important means to ensure PI Subjects' right to know, and an important mechanism that restricts the PI Controller' behavior and cooperates with supervision and administration. PI protection policies shall clearly, accurately and completely describe how the PI Controller processes PI. Table D.1 shows a template of PI protection policy.

Table D.1 Template of PI Protection Policy

PI protection policy template	Compiling Requirements
This Policy only applies to the product(s) or service(s) of XXXXX, including XXXX, XXXX, XXXX, and XXXX. Latest update: XX/XXXX (Month/Year) Please contact us using the details below if you have any doubt, comment or suggestion: E-mail: Tel.: Fax:	This section is the scope of application, including the scope of products, services and the PI Subjects that the PI Protection Policy applies to, period of effectiveness, and time of update.
This Policy will help you better understand the following: ✓ Rules for the collection and use of PI for business function 1; ✓ Rules for the collection and use of PI for business function 2; ✓ …… ✓ How we protect your PI; ✓ Your rights; Your rights ✓ How we process children's PI; ✓ How your PI is transferred worldwide; ✓ How this Policy will be updated; ✓ How to contact us. XXXX understands the importance of PI to you and will do our best to ensure the security and reliability of your PI. We are committed to maintaining your trust in us and sticking to the following principles to protect your PI: principle of consistency between rights and responsibilities, principle of clear purpose, principle of optional consent, principle of minimum necessary, principle of security assurance, principle of subject participation, and principle of openness and transparency. In the meantime, XXXX hereby promises that we will take security measures to protect your PI according to mature standards of the industry. Please read carefully and understand this PI Protection Policy before using our product/service.	This section lists the key points of the PI Protection Policy. The objective is to enable PI Subjects to quickly get hold of the main components of the PI Protection Policy and the core ideas of the Controller's statement.

Table D.1 (continued)

PI protection policy template	Compiling Requirements
■ **Rules for the collection and use of PI for business function 1** **1. What kind of PI we collect about you** ● The business functions we provide require some information to run. If you choose to use this business function, you will need to provide us with or allow us to collect the essential information including: ... A total of XX types of PI. ● You may choose, at your discretion, whether to provide us with or allow us to collect the following information: ... A total of XX types of PI. Such information is not essential for the delivery of the business function, but it is important to improve the quality of service, develop new products or services, etc. We will not force you to provide this information, and your refusal will not adversely affect the use of the business functions. When you use this business function, our APP will request the following permissions to access PI in the system: ... A total of XX permissions. If you do not authorize, we will be unable to provide this business function. Except the permissions above, you can choose whether to grant additional system permissions to our APP. **2. How we use your PI** ● For essential PI, we will use it to provide the business functions including ... We also use such information to maintain and improve this business function and develop new business functions, etc. ● For non-essential PI, we will use it for the following purposes, including … **3. How we entrust the processing, sharing, transfer and publicly disclosure of your PI** **(1) Entrustment of processing** Certain specific modules or sub-functions of this business function are provided by external vendors. For example, we engage external service providers to assist us in providing customer support. We will sign strict confidential agreements with the companies, organizations and individuals to whom we entrust the processing of PI, which will bind them to processing the PI in accordance with our requirements, this PI Protection Policy and other relevant confidentiality and security measures. **(2) Sharing** We will not share your PI with any company, organization or individual other than our Company, unless with your explicit consent. At present, we will seek your consent to the sharing of your PI in the following scenarios: a) …… To learn about the companies, organizations, and individuals currently involved in this scenario, click here【Provide a hyperlink】. b) …… To learn about the companies, organizations, and individuals currently involved in this scenario, click here【Provide a hyperlink】 c) …… To learn about the companies, organizations, and individuals currently involved in this scenario, click here【Provide a hyperlink】 We might share your information as stipulated by laws, regulations or the mandatory requirements of government agencies. **(3) Transfer** We will not transfer your PI to any company, organization, or individual except under the following circumstances: a) Transfer with explicit consent: after acquiring your explicit consent, we will transfer your PI to other parties; b) When the transfer of PI is involved in a(n) merger, acquisition or bankruptcy liquidation, we will require the new company or organization to which your PI is transferred to continue to be bound by this PI Protection Policy, otherwise we will require the new company or organization to seek your consent again. **(4) Public Disclosure** We will only publicly disclose your PI under the following circumstances: a) After we obtain your explicit consent; b) Statutory disclosure: we might publicly disclose your PI as stipulated by laws, regulations or the mandatory requirements of government agencies.	1. List the purposes for collecting and using PI in detail; do not use generalized language. 2. List the types of PI in detail for different business functions. 3. Clearly state the types of PI that are essential to specific business functions. 4. When collecting information of legal documents such as ID card, passport, driver's license and personal biometric information, the specific information involved in the collection shall be brought to the notice of the PI Subjects, and the purposes and rules of processing such information shall be explained. 5. Do not use ambiguous language to describe the information to be collected, for instance, "we will collect your identity related information". Instead, it shall be clearly stated that "we will collect the information of your name, telephone number and address." 6. State the geographic areas involved in the use of PI, e.g. storage and backup locations of PI, areas involved in the transmission of PI; if cross-border transmission of PI is involved, it shall be separately listed or highlighted. 7. State the estimated retention time (e.g. 5 years from the date of collection) and the date of data deletion or destruction (e.g. Dec.31st 2019 or when the PI Subject de-registers) for different types of PI based on use conditions. 8. Promise to re-seek the consent of the PI Subjects when it is indeed necessary to change the purpose for collection and use of the information. 9. PI Controllers shall state whether the PI needs to be shared or transferred, and if so, clearly state the types of the PI to be shared or transferred, the reasons of such sharing and transfer, the recipient of the PI, the restrictions and administration rules for the recipient, the recipient's use purpose of the PI, the security measures adopted during the sharing and transfer of the PI, and whether the sharing and transfer of PI could bring high risks to the PI Subjects. 10. State whether the PI needs to be publicly disclosed, and describe the types of PI to be publicly disclosed, the reason for such public disclosure, and whether such disclosure could bring high risks to the PI Subjects. 11. State the circumstances under which the PI Controller can share, transfer and publicly disclose data without PI Subjects' prior consent. For example, responding to requirements of law reinforcement authorities and government agencies, conducting PI security audits, and protecting PI Subjects from fraud and severe personal injuries.

Table D.1 (continued)

PI protection policy template	**Compiling Requirements**
■ **Rules for the collection and use of PI for business function 2** **Omitted.**	—
■ **How we protect your PI** I. We have employed security protection measures according to industry standards to protect your PI, prevent unauthorized access to, disclosure, use, modification, damage or loss of data. We will take every practical measure to protect your PI. For instance, … II. We have acquired the following certificates: ... III. Our data security capability includes: IV. We will take all reasonable and practical measures to ensure that unnecessary PI are not collected. We will only retain your PI for the period necessary to deliver the purposes stated in this Policy, unless the extended retention is required or allowed by laws. V. We will regularly update and publicize reports on security risks, PI impact assessment, etc. You can access these by ... VI. The network environment is not 100% secure. We will do our utmost to ensure or guarantee the security of any information you send to us. If your legal rights and benefits are adversely affected due to the unauthorized access to, disclosure, tampering or damage of your PI resulting from the damage of our physical, technical or management protection facilities, we will assume legal liabilities accordingly. VII. In the case of an unfortunate PI security incident, we will, in a timely manner and in accordance with laws and regulations, inform you of the basic conditions and possible impacts of the security incident, response measures that are already taken or to be taken by us, suggestions for you regarding self-prevention and risk mitigation, our remedial measures for you, etc. We will inform you of such information by email, fax, telephone, push notification, etc., and when it is difficult to notify each PI Subject individually, we will properly and effectively issue a public notice. At the same time, we will also take the initiative to report the handling of PI security incidents in accordance with regulatory requirements.	1. Clearly state the PI Controller’s security measures for PI, including but not limited to measures to protect the integrity of PI, encryption measures during transmission, storage and backup of PI, authorization and audit mechanism for access and use of PI, and retention and deletion mechanism for PI. 2. The PI security agreements that the PI Controller is complying with and certifications it has obtained, including international or domestic laws, regulations, standards and agreements on PI security that are proactively observed by the PI Controller, as well as PI security certifications the PI Controller has obtained from independent and competent certification agencies. 3. State possible security risks after providing PI. 4. State that the PI Controller will assume legal liabilities in case of a PI security incident. 5. State that PI Subjects will be informed without delay in case of a PI security incident.

Table D.1 (continued)

PI protection policy template	Compiling Requirements
Your rights According to relevant laws, regulations and standards in China, as well as common practices in other countries and regions, we will ensure your following rights to your PI: **(1) Access your PI** You have the right to access your PI, unless laws and regulations specify otherwise. If you wish to access your data, you can do so by: …… If you cannot access the PI via the links above, you can use our Web form or send an email to XXXX at any time. We will respond to your access request in 30 days. As for other PI generated during your use of our products or services, we will provide you with access to such information as long as no excessive input is required. If you wish to access such data, please send an email to XXXX. **(2) Rectify your PI** When you find a mistake in your information that we are processing, you have the right to ask us to rectify it. You can submit a rectification request through the channels listed in "(I) Access your PI". If you cannot rectify the PI via the links above, you can use our Web form or send an email to XXXX at any time. We will respond to your rectification request within 30 days. **(3) Delete your PI** You can submit a request to delete your PI to us under the following circumstances: 1. If our processing of PI violates laws or regulations; 2. If we collected and used your PI without your consent; 3. If our processing of PI breaches our agreement with you; 4. If you no longer use our products or services or you have cancelled your account; 5. If we no longer provide you with products or services. When we decide to respond to your deletion request, we will also inform the entity that acquires your PI from us and ask it to delete your PI without delay, unless otherwise specified in laws and regulations, or the entity has acquired specific authorization from you. When you delete the information from our services, we might not immediately delete the corresponding information from our backup system, but will delete it when the backup system is updated. **(4) Change the scope of your consent** Each business function needs some basic PI to be completed. As to the collection and use of additional PI, you can give or withdraw your consent at any time. You can do so by: …… …… When you withdraw your consent, we will stop processing the corresponding PI. However, your withdrawal of consent will not affect the processing of PI carried out based on your prior consent. If you do not wish to receive our business promotion ads, you can unsubscribe at any time by: …… **(5) De-register** You can de-register at any time by: …… After de-registration, we will stop providing you with any product and service and delete your PI according to you request, unless laws and	1. State PI Subjects' rights in terms of their PI, including but not limited to: the range of PI over which a PI Subject has a choice in the collection, use and public disclosure, the PI Subject's control of access to, rectification, deletion, acquirement of PI, the PI Subject's privacy preference settings, communication and advertisement preferences the PI Subject can choose, channels for the PI Subject to deactivate services and de-register, effective channels for the PI Subject to safeguard legal rights. 2. When self-configuration or operation (e.g. configuration and operation of software, browser, and mobile terminal) is required in order to access, rectify, delete PI or withdraw consent, the PI Controller shall clearly state the configuration and operation process in detail. The statement should be easy for PI Subjects to understand, and channels for technical support (such as customer service hotline and online customer service) should be provided when necessary. 3. If expense is incurred during a PI Subject's exercise of his/her rights, the reason and basis for charging should be clearly stated. 4. If it takes long to respond to the request of a PI Subject exercising his/her rights, the response time and the reason for not being able to respond within a short time should be clearly stated. 5. If re-authentication is needed during a PI Subject's exercise of his/her rights, the reason for such authentication should be clearly stated, and proper control measures should be taken to prevent leakage of PI during the authentication. 6. If the PI Controller rejects a PI Subject's request to access, rectify, delete the PI or withdraw consent, the reason and basis of such rejection should be clearly stated.

PI protection policy template	Compiling Requirements
regulations specify otherwise. **(6) Acquisition of a copy of PI by PI Subjects** You have the right to obtain a copy of your PI by: …… When it is technologically feasible, e.g. with matched data interface, we can directly transmit the copy of your PI to the third party designated by you according to your request. **(7) Restrict automated decision-making by information system** For some business functions, decisions are made solely based on an automated decision-making mechanism such as information system and algorithm. If these decisions significantly affect your legal rights and interests, you have the right to ask for our explanation and we will make proper remedies. **(8) Respond to your above-mentioned requests** For security, you might be required to submit written requests or prove your identity by other means. We might ask you to verify your identity before handling your request. We will respond in 30 days. If you are not satisfied, you can file a complaint by: …… We will not charge you for your reasonable requests in principle. However, a fee to reflect the cost will be imposed as appropriate on repeated requests beyond reasonable scope. As for repeated requests that are groundless and need excessive technological means (e.g. developing a new system or fundamentally changing the current practices) to fulfill, bring about risks to others' legitimate rights and interests or are downright impractical (e.g. involving information stored on a backup disk), we might reject. We will not be able to respond to your request under the following circumstances: 1. Related to our compliance with the obligations under the laws and regulations; 2. Directly related to national security or defense security; 3. Directly related to public security, public health or major public interests; 4. Directly related to criminal investigations, prosecutions, trials and enforcement of court decisions, etc.; 5. We have sufficient proof that you have subjective malice or abuse of rights； 6. For the purpose of safeguarding your life, property and other important legal rights and interests or those of other individuals but it is difficult to obtain consent; 7. Responding to your request will cause serious harm to your legitimate rights and interests, or those of other individuals or organizations. 8. Involving trade secrets.	

Table D.1 (continued)

PI protection policy template	Compiling Requirements
How we process children's PI Our products, websites and services are mainly adult oriented. A child should not create his/her own account without consent of his/her parents or guardians. Children's PI that is collected with their parents' consent will only be used or publicly disclosed when it is permitted by laws, explicitly consented to by their parents or guardians, or is essential to protecting the children. Although the definition of children varies in local laws and customs, we regard anyone below 14 years old as a child. If we find that a child's PI has been collected without his/her parents' prior consent, we will delete relevant data as soon as possible.	—
How your PI is transmitted worldwide In principle, the PI we collect and generate in the territory of the People's Republic of China will be stored within the People's Republic of China. We provide products or services based on our resources and servers worldwide, that is to say, with your consent, your PI might be transmitted to or accessed from a jurisdiction outside of the country/region where your products or services are located. Such jurisdiction might have a different data protection law, or even no relevant laws. Under such circumstances, we will ensure that your PI will enjoy the same level of protection as it does in the People's Republic of China. For instance, we will ask you for your consent to the cross-border transmission of your PI, or employ data de-identification and other security measures before the cross-border transmission of data.	If cross-border transmission of information is required by business needs or government or judicial supervisions, the PI Controller needs to clearly state the types of data to be transmitted across border and the standards, agreements and legal instruments (such as contracts) the cross-border transmission shall be bound by.
How this Policy will be updated Our PI Protection Policy might be changed. We will not reduce any of your rights under this PI Protection Policy without your explicit consent. We will release any change to the Policy on this page. For major changes, we will provide a more conspicuous notice (including, for certain services, notices via email that explains the details of the changes to the PI Protection Policy). The major changes to this Policy include but are not limited to: 1. Major changes in our service mode, e.g. the purpose of processing PI, the type of processed PI, and how PI is used; 2. Major changes in our ownership structure, organizational structure, e.g. the change of owners due to business adjustments, a(n) bankruptcy, merger and acquisition. 3. Changes of the main object which PI is publicly disclosed to, shared with, or transferred to; 4. Changes in your rights involved in PI processing and in how you exercise such rights; 5. Changes of our responsible department, contacts and complaint channels for PI protection; 6. When a PI impact assessment report indicates high risks. We will also archive the old versions of this Policy for your reference.	When there is a major change to the PI protection policy, the PI Controller needs to update the PI protection policy in time and state the means to inform PI Subjects without delay. Generally, the followings means can be used to inform the PI Subjects: notifying the PI Subjects when they log into the information system, updating the information system and notifying the PI Subjects with a pop-out window during their use of the information system, directly sending a push notification to the PI Subjects when they are using the information system, sending an email or a text message to the PI Subjects, etc.

Table D.1 (continued)

PI protection policy template	Compiling Requirements
How to contact us If you have any doubt, comment or suggestion regarding this Policy, please contact us via: ...... We have set up a dedicated department for PI protection (or a PI protection officer) that you can contact via: ...... Generally, we will reply to you in 30 days. If you are not satisfied with our reply, especially if our processing of PI hurts your legal rights and interests, you can seek solutions through the following external channels:	1. PI Controllers need to clearly state the channels for PI security related feedbacks and complaints, e.g. contacts, address and email address of the department responsible for PI security, the form for PI Subjects to report problems, and clearly state the time frame within which the PI Subjects can expect a reply. 2. PI Controllers need to state the external dispute resolution body and its contacts in case of any dispute or conflict that cannot be resolved through negotiation with a PI Subject. The external dispute resolution body usually can be courts in the jurisdiction where the PI Controller is located, independent institutions that certify the PI protection policy of the PI Controller, and industry self-regulation associations and relevant government agencies.

Bibliography

[1] GB/Z 28828—2012 Information security technology-Guideline for personal information protection within information system for public and commercial services

[2] GB/T 32921—2016 Information security technology—Security criterion on supplier conduct of information technology products

[3] Cybersecurity Law of the People's Republic of China (adopted at the 24th Session of the Standing Committee of the 12th National People's Congress on Nov. 7th 2016)

[4] Decision of the Standing Committee of the National People's Congress on Preserving Computer Network Security (adopted at the 19th Session of the Standing Committee of the 9th National People's Congress on Dec. 28th 2000)

[5] Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection (adopted at the 30th Session of the Standing Committee of the 11th National People's Congress on Dec. 28th 2012)

[6] E-Commerce Law of the People's Republic of China (adopted at the 5th Session of the Standing Committee of 13th National People's Congress on Aug. 31st 2018)

[7] Provisions on the Protection of PI of Telecommunications and Internet Users (Order No.24 of the Ministry of Industry and Information Technology released on Jul. 16th 2013)

[8] Seventh Amendment of the Criminal Law of the People's Republic of China (adopted at the 7th Session of the Standing Committee of the 11th National People's Congress on Feb. 28th 2009)

[9] Ninth Amendment of the Criminal Law of the People's Republic of China (adopted at the 16th Session of the Standing Committee of the 12th National People's Congress on Aug. 29th 2015)

[10] Emergency Response Plan for National Cybersecurity Incidents (Document [2017] No.4 issued by Cyberspace Administration of China on Jan. 10th 2017)

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

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

[13] ISO/IEC 29134:2017 Information technology - Security techniques – Guidelines for privacy impact assessment

[14] ISO/IEC 29151:2017 Information technology - Security techniques – Code of practice for personally identifiable information protection

[15] ISO/IEC DIS 29184 Information technology – Online privacy notices and consent

[16] APEC Privacy Framework, APEC, 2005

[17] Consumer Privacy Bill of Rights Act of 2015 (Administration Discussion Draft), White House, 2015

[18] CWA 16113:2012 Personal data protection good practices

[19] EU General Data Protection Regulation, 2015

[20] EU-U.S. Privacy Shield, 2016

[21] NIST SP 800-53 Rev. 4:2013 Security and privacy controls for federal information systems and organizations

[22] NIST SP800-122:2010 Guide to protecting the confidentiality of personally identifiable information (PII)

[23] NISTIR 8062:2017 An introduction to privacy engineering and risk management for federal systems

[24] The OECD Privacy Framework, OECD, 2013