GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GB/T 40660-2021

Information security technology - General requirements of biometric information protection

信息安全技术 生物特征识别信息保护基本要求

Issued on: October 11, 2021 **Implemented on: May 01, 2022**

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

Table of Contents

Information security technology - General requirements of biometric information protection

1 Scope

This document stipulates the basic principles and security requirements that various types of biometric information controllers shall follow when conducting biometric information processing activities such as collection, storage, use, entrusted processing, sharing, transfer, public disclosure and deletion.

This document applies to the regulation of biometric information processing activities carried out by various types of biometric information controllers, as well as the evaluation of biometric information processing activities carried out by third-party organizations.

2 Normative references

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

GB/T 25069, Information security technology - Glossary

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

3 Terms and definitions

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

3.1 Biometric original information

Analog or digital representations of physical, biological or behavioral characteristics of natural persons obtained through acquisition, preprocessing, etc.

Note: e.g., samples, images.

3.2 Biometric comparison information

Information – obtained through technical processing of the biometric original information – that is used for comparison during the identification process.

3.3 Biometric information

Personal information – obtained through technical processing of a natural person's physical, biological or behavioral characteristics – that can be used for identifying the natural person either alone or in combination with other information.

Note 1: Biometric information includes personal facial recognition features, irises, fingerprints, genes, voice prints, gait, palm prints, auricles, eye prints, etc.

Note 2: Biometric information includes biometric original information and biometric comparison information.

3.4 Biometric information subject

Natural person identified by or associated with biometric information.

3.5 Biometric information controller

Organization or individual that has the ability to determine the purpose and method of processing biometric information.

3.6 Revoke

Prevent specific biometric comparison information and corresponding identity-related information from being verified.

Note: A biometric information subject may be rejected because it has been added to a revoke list.

3.7 Irreversibility

A characteristic that the corresponding biometric original information cannot be deduced from the biometric comparison information.

3.8 Unlinkability

An attribute that two or more biometric comparison information cannot be linked to each other.

Note: With unlinkability, a user can use different programs, resources and services multiple times, and others cannot link these uses together through biometric comparison information.

c) Collection of biometric information that does not belong to the biometric information subject – including biometric original information – shall be avoided.

d) Obtaining information from non-biometric information subjects by indirect means shall be avoided.

e) The biometric information subject who cannot finish the information collection shall be informed of the subsequent alternative processing procedures available.

f) When collecting biometric information in accordance with relevant national laws and regulations, etc., the biometric information subject shall be informed of the relevant requirements and the type of biometric information collected.

g) The risk of presented interference and attacks shall be fully considered. Considerations include but are not limited to different attack forms such as physical and virtual, different attack materials such as paper and plastic, and different attack environments such as presentation angles and light conditions.

6 Storage of biometric information

The requirements for the biometric information controller are as follows.

a) The biometric information and the identity-related information of the biometric information subject shall be stored by means of technical isolation.

Note 1: Isolation methods include logical isolation, physical isolation, etc.

b) When biometric information is stored, its irreversibility shall be ensured.

c) In principle, the biometric original information shall not be stored directly, and the measures that can be taken include but are not limited to:

1) storing only the summary information of the biometric information;

2) realizing functions such as identification and authentication by directly using biometric information in the collection terminal;

3) deleting the biometric original information after using facial recognition features, fingerprints, palm prints, iris, etc. to realize functions such as identity recognition and authentication.

Note 2: Summary information is usually irreversible.

Note 3: Except for situations related to the fulfillment of obligations stipulated by laws and regulations by the biometric information subject.

d) A diversification process shall be used to support the generation of updatable and revocable biometric comparison information:

1) The biometric comparison information generated during the diversification process shall be irreversible;

2) The biometric comparison information of the same biometric information subject generated through the diversification process shall be unlinkable.

Note 4: The diversification process refers to transforming single or multiple biometric original information of a biometric information subject into multiple independent biometric comparison information, which is used for updating biometric comparison information or providing independent biometric comparison information for different applications.

e) When storing biometric comparison information, the risk of data breath shall be fully considered and safe processing shall be carried out. Mechanisms that can be used include but are not limited to:

1) Carry out security protection through logical and physical means, by storing biometric comparison information on personal tokens or cards;

2) Perform encryption operations using a key known only to the biometric information controller or the biometric information subject;

3) Minimize the stored biometric comparison information;

4) Use identifiers that cannot be directly linked to the biometric information subject.

f) The unlinkability of biometric comparison information between applications or databases shall be maintained to prevent the biometric comparison information from being used to link different applications in the same database or the same information subject in different databases. Unlinkability can be obtained through a combination of the following mechanisms:

1) using different keys or mechanisms between applications to encrypt biometric comparison information to prevent links to biometric information subjects. In principle, different keys shall be kept by different personnel;

2) using the following methods or combinations thereof between applications: using different biometric modes, using incompatible feature extraction algorithms, using incompatible biometric data exchange formats.

g) Copies of biometric information, such as backup information, archive information, etc., shall be stored with the same protection measures as the information being copied.

h) Only the minimum biometric information required to meet the purpose of authorization and consent of the biometric information subject shall be stored.

necessary to achieve the purpose of authorized consent; the operation of specific personnel shall be specified; the safety of the operation process shall be ensured; the operator's authority shall be promptly withdrawn.

8 Rights of biometric information subject

The requirements for the biometric information controller are as follows.

a) The biometric information subject shall be provided with the method of querying the following information:

1) type of biometric information of the biometric information subject;

2) authorization and consent of biometric information, including but not limited to the method and date of obtaining authorization, authorized collection and use purposes, and authorized storage time;

3) processing of the biometric information;

4) security incidents, such as being tampered with, leaked, of the biometric information.

b) The following requests of the biometric information subject shall be responded in a timely manner:

1) modifying or withdrawing the authorization of its biometric information;

2) updating the biometric information.

c) Biometric information shall be deleted or anonymized in a timely manner when one of the following conditions is met:

1) The authorized storage period of biometric information has expired;

2) The biometric information subject withdraws the authorization for the biometric information;

3) The purpose of using the biometric information authorized by the biometric information subject has been achieved or determined to be unnecessary.

d) A list of biometric information to be deleted or anonymized shall be established based on the authorized storage period of biometric information and other information.

e) The procedures and safeguards for deleting and anonymizing biometric information shall be clarified to ensure complete and safe processing of biometric information.

11 Requirements for biometric information security management

The management requirements for the biometric information controller are as follows.

a) When providing multiple alternative identification methods, the biometric information should not be used as the default option for initial settings.

b) Security risk-related assessments shall be carried out continuously, measures to reduce processing risks shall be taken timely to fully protect the rights of biometric identification subjects, including:

1) Before planning the collection of biometric information for business activities, the necessity of using biometric information – and whether there are corresponding security capabilities and security control measures – shall be evaluated;

2) Before collecting biometric information, a personal information security impact assessment shall be conducted to ensure that the risk of processing biometric information is controllable;

3) Before performing actions such as changing the purpose or scope of biometric information processing, entrusting a third party to process, share or transfer, etc., a personal information security impact assessment shall be conducted to ensure that no new security risks are introduced;

4) Where there is sharing and transfer of biometric information, the necessity of sharing and transferring biometric information shall be regularly assessed;

5) The existing biometric information processing should be re-evaluated on a regular basis (such as every year) to ensure that existing security measures meet current security requirements.

c) Records of biometric information processing activities shall be established and maintained, and the contents of the records should include:

1) type and source of the controlled biometric information;

2) authorization of biometric information;

3) processing of biometric information.

d) Protection plans shall be formulated for biometric information of different types and processing stages, and the protection plans should be disclosed to relevant biometric information subjects.

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

Full-copy PDF can be purchased from 1 of 3 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

3. https://www.google.com/search?tbm=bks&q=ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Google Books -- Select your currency.
- Processed by Google (delivery, tax invoice etc.). Delivered in 9 seconds by Google.
- Tips: Download an unprotected True-PDF (text-editable) from Google-Books:
  1. https://play.google.com/books → 2. Sign in → Google account
  3. Find the BOOK you bought → 4. Click "3-dots" → Export
  5. Save as "*.pdf" (Save True-PDF to your local computer for offline reading/printing)

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

Accountable person and shareholder: Wayne Zheng

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

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