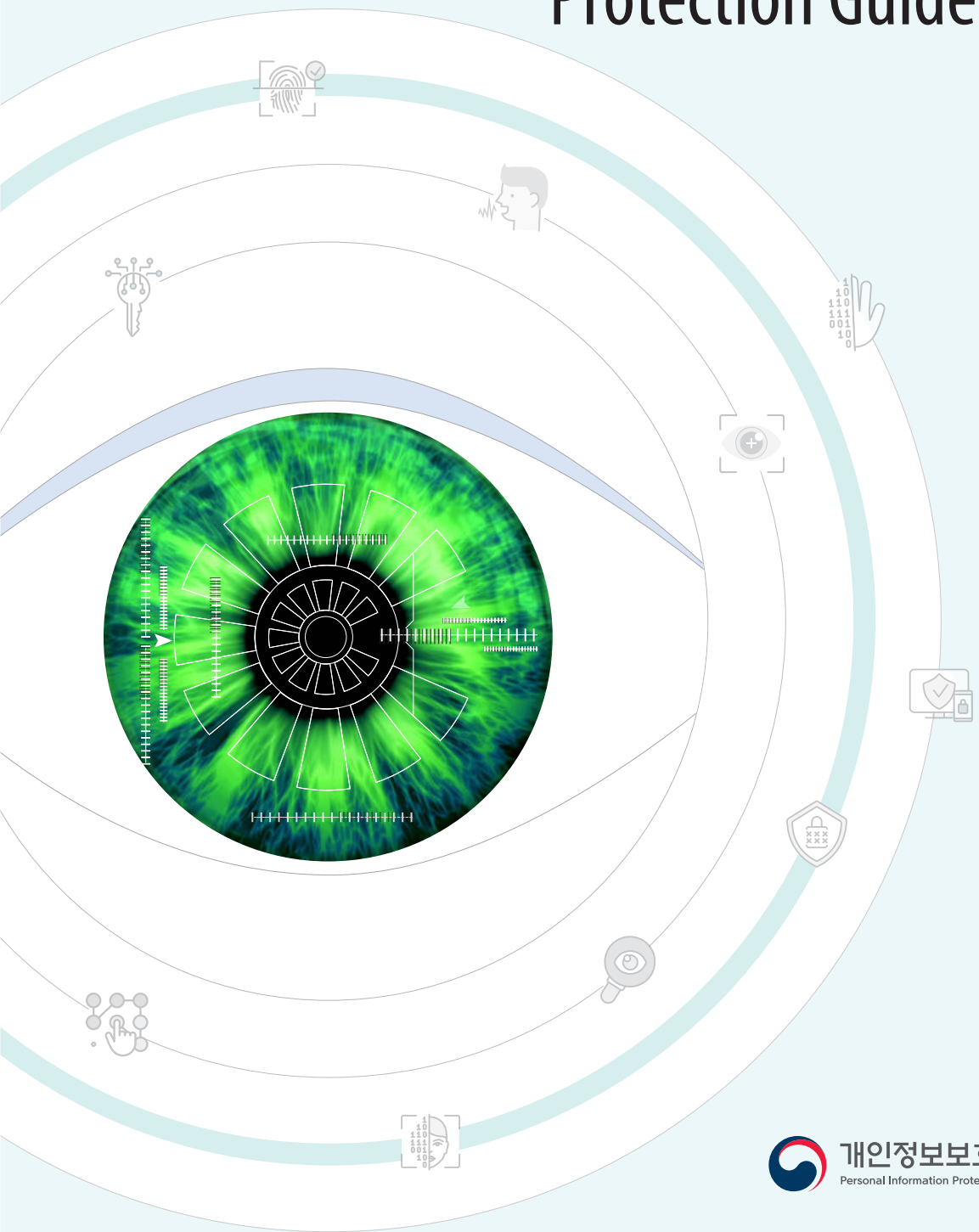
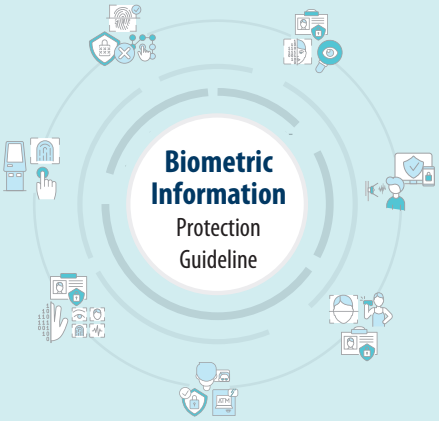
September 2021

Biometric Information
Protection Guideline



개인정보보호위원회
Personal Information Protection Commission


Biometric
Information
Protection
Guideline

CONTENTS

Overview

1 Biometric Information Trends

- The use of biometric information was previously limited to an enterprise access control system. However, its application has been increasing even to information communication areas including unlocking of smartphones and AI-based voice assistant service.
  - ※ **The global biometric market size is expected to increase with an average growth of 22.7 percent from about USD 2.4 billion in 2016 to around USD 15.1 billion. (Statista, 2020)**
  - ※ **The Korean biometric market size has recorded an average growth rate of 8.13 percent. It increased from KRW 261.7 billion in 2018 to KRW 357.7 billion in 2021. (Boannews, Security World, 2020 global security market outlook report)**
  - The use of biometric information in various sectors has become common since devices using biometric information are widely spread and the transition to contactless services has increased due to the COVID-19 situation.

- Simultaneously, public concern is also rising since leaks and forgery of biometric information have been occurring recently.

Case 1 An Israeli security specialist detected unencrypted information including username, password, fingerprint, and facial information in the "server revealed to the internet due to an improper security setting" of a biometric information related manufacturer. (Aug 2019)

Case 2 Army surgeons made fake silicone fingerprintsof their commanding officer and received overtime pay by using the fake fingerprints in a fingerprint reader for checking attendance. (Mar 2019)

Case 3 The DB of a U.S. federal department was subjected to an advanced persistent attack (APT) by a hacker group. Accordingly, the personal information of 22 million former and current civil servants were leaked, along with the fingerprint information for 5.6 million of them. (Jun 2015)

- In response to such cases, major countries including the EU specifically defined "biometric information" as a type of personal information and announced guidelines including biometric information protection principles.

Biometric Information Protection Guidelines of Foreign Countries

Country and Institution	Guideline
Polish data protection authority (UODO)	• Guideline on the use of biometric information (2021)
Office of the Privacy Commissioner for Personal Data (PCPD)	• Guidance on Collection and Use of Biometric Data (2020)
European Data Protection Board (EDPB)	• Guidelines on processing of personal data through video devices (Mar 2019) • Opinion on developments in biometric technologies(Mar 2012)
Australian Human Rights Commission (AHRC)	• Human Rights and Technologies (2019)
Commissioner for Privacy and Data Protection (CPDP)	• Biometrics and privacy (2016)
Biometrics Institute	• Biometrics Privacy Guidelines (2015)
International Biometrics & Identification Association (IBIA)	• Recommendations of IBIA Privacy Best Practice for Commercial Use of Biometric Information (2014)
Cross Government Biometrics Group (CGBG)	• Guiding Principles on the Use of Biometric Technologies (2009)

2 Objective

- As authentication and identification services are increasing with the use of biometric information in various sectors, including the use of fingerprints and iris scanning when unlocking smartphones, facial recognition when controlling access, and voice-based AI when providing assistant service:
  - We aim at clarifying the concept and scope of biometric information prescribed in the current personal information protection ordinance and related notice.
  - We also attempt to form a basis to safely apply biometric information by specifically suggesting basic principles for the biometric information protection and protection measures for each phase.

※ **We revised and improved the existing 「Biometric Information Protection Guideline」 (Dec 2017) with *the personal information protection ordinance amended in August 2020.**

* According to Paragraph 3 Article 18 of the ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT, the following information is prescribed as sensitive information: "Personal information resulting from specific technical processing of data relating to the physical, physiological, or behavioral features of an individual for the purpose of uniquely identifying that individual"

3 Concept of Biometric Information

A. Definition of Bio and Biometric Information

(1) "Bio information" means information on the ①physical, biological, and behavioral features of a person including fingerprints, face, irises, veins, voice, and handwriting. Thus, it is used in ②authenticating and identifying a specific person or processed through processed through certain technical means ③ to understand a person's features (age, gender, emotion, etc.).

① Physical, biological, and behavioral features of a person

- Physical: fingerprints, face, blood vessel's shape of iris and retina, vein's shape of palms and fingers, palm prints, and the shape of earflaps t, etc.
- Biological: brain waves, electrocardiogram, genetic information, etc.
- Behavioral: voice, handwriting, gaits, interval and speed of typing, etc.

② **To authenticate and identify a certain person:** Use (compare and contrast) features extracted from one's fingerprints, iris, and face.

i) Authentication: Verify one's identity by comparing the bio information entered by the user with that stored in devices to check whether the individual has the privilege to use an applicable service.

※ **For example, an access control system allows access by verifying one's identity after one's fingerprints are registered.**

ii) Identification: Identify a specific person among several people by comparing the individual's bio information with a lot of information stored in the DB where individual bio information is stored.

※ **For example, an AI speaker gives answers by identifying a member whom it is talking with among other family members whose voices are registered.**

③ **To understand features of a person:** Check or categorize a status (age, gender, and emotion) of a person not for the purpose of authentication and identification.

※ **Example 1: Behavior of classifying users by predicting their age or gender through facial recognition**

※ **Example 2: Behavior of layering a sticker on a user's face to the position of their eyes, nose, and lips through automatic facial recognition**

④ **Processing with certain technical means:** The entire process of electronically handling information for either authenticating and identifying a person or comprehending a person's features by collecting and registering original information including images through a sensor input device and extracting features from the original information.

(2) "Biometric information" means information processed for authenticating and identifying a certain person with that person's bio information.

➜ Thus, bio information is composed of **"biometric information"** processed for authenticating and identifying a certain person and **"general bio information"** processed to learn features (age, gender, emotion, etc.) of a person.

Note Classification and example of biometric and general bio information

- **Picture (video) of a face**
  - **Biometric information**: It is used to authenticate and identify a person by technically extracting features of the person's face picture (video) to use the information for the access control (facial recognition) system.
  - **General bio information**: It is used to understand gender and emotional status (happy, angry, etc.), even though a person's features are technically extracted from the person's face picture (video).
- **Voice**
  - **Biometric information**: When responding to a person by identifying the person whom an AI speaker is talking with by technically extracting the features of the person whose voice is registered in the speaker.
  - **General bio information**: When using the information not for identification but for understanding a person's emotional status (angry or joyful voice, etc.), even though features of the person are technically extracted from the AI speaker where their voice is registered.

B. Classification of Biometric Information

(1) Biometric information is divided into original biometric information ("original information") collected and entered through an input device for the purpose of authenticating or identifying a person and biometric feature information ("feature information") created through a certain technical means extracting one's features.

① When original information is either leaked or misused/abused in the process of electronically treating biometric information, there is a high risk of personal information infringement.

- When encoding original information to store it safely or keeping it even after generating feature information, this requires a protection measure including keeping it separately from other personal information.

※ **Refer to 4. 4.Storage/Disposal Phase of III Protection Measures for Biometric Information.**

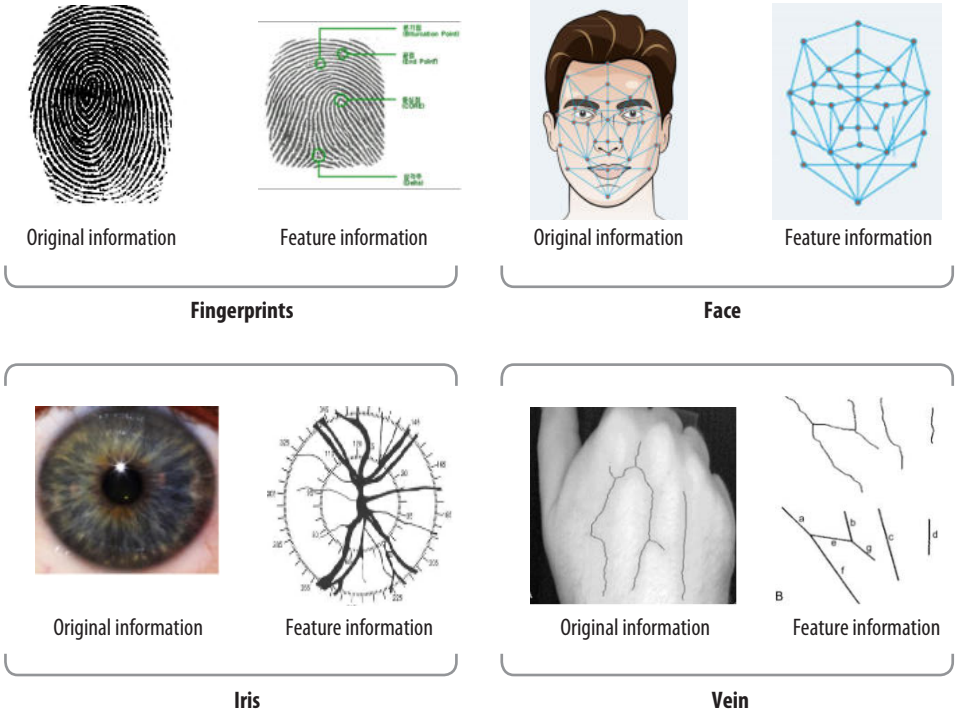
② Feature information is applicable to sensitive information according to *Paragraph 3 Article 18 of the ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT.

* "Personal information resulting from specific technical processing of data relating to the physical, physiological, or behavioral features of a person for the purpose of uniquely identifying that individual"

- Thus, feature information is *regulated by Article 23 (Limitation to Processing of Sensitive Information) of the PERSONAL INFORMATION PROTECTION ACT.

  * "A personal information handler shall be able to process information only when obtaining the consent of the data subject apart from the consent to the processing of other personal information or where other statutes require or permit the processing of sensitive information."

Example of original and feature information



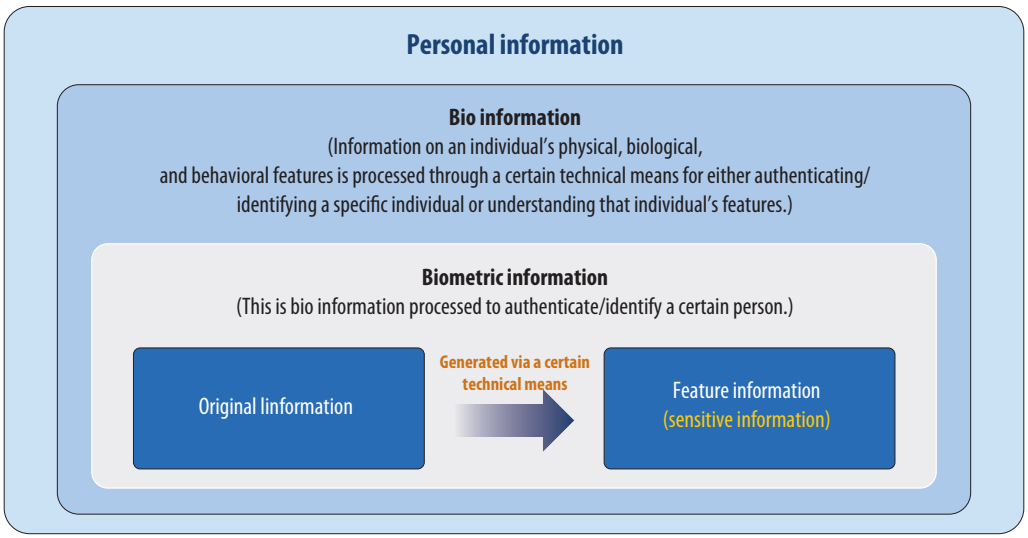
※ Source: scienceDirect.com

C. Relation among Personal, Bio, and Biometric Information and Applicable Rules

(1) When information on a person's physical, biological, and behavioral features isn't technically processed for authentication/identification purposes or understanding of the person's features, the information is applicable to general personal information.

※ **For example, general face pictures, audio files, and other info can be collected for the purpose of reading/storage**

- The information technically processed to figure out an individual's features (age, gender, emotion, etc.) besides authentication/identification purposes falls under general bio information, not biometric information.



Classification		Definition
Personal information		It is possible to identify a certain person with the information itself or it is information can be comprehensible by easily aggregating with other information
Bio information		Information on an individual's physical, biological, and behavioral features is **processed through a certain technical means to either authenticating/identifying a specific individual or understanding the individual's features (age, gender, emotion, etc.)**.
Biometric information		This is a person's bio information that is processed **to authenticate/identify a certain person**.
	Original information	This biometric information is **used in creating feature information**, collected and entered via an input device.
	Feature information	Information **created through a certain technical means**, extracting features from original information

(2) Protection principles suggested in this Guideline and protection measures for each phase are applied to biometric information.

- It is not obligated to encode "general bio information" applied to biometric information when storing it or to keep it separately when keeping original information.
- However, it is recommended to conduct protection measures on general bio information at a level equivalent to those of biometric information by considering personal information infringement risk when the applicable information is leaked or misused/abused during its collection, transmission, and storage.

※ **Refer to Protection Measures Recommended for General Bio Information of Appendix 3.**

(3) When using general face picture/video, audio files, and other data later in generating feature information with authentication/identification purposes, the applicable information is considered biometric information. Thus, a protection measure applied to biometric information shall be conducted.

Note Case of using general personal information in creating feature information

- When registering a face picture photographed with a camera into a human resource (HR) management system for HR management, the face picture is considered general personal information.
- If a facial recognition system is to be introduced later, then the picture already stored in the HR system can be used in extracting feature information of the picture without newly collecting face pictures from users.
  - In this case, the collected picture is being used for other purposes different from the original purpose. Thus, the information handler shall legally obtain consent to the collection and use of biometric information before enacting the plan to use that info in extracting feature information.
  - The handler shall also implement protection measures applied to biometric information suggested in this Guideline.

Upload to the HR system.

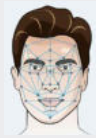
HR system

	Name	Hong Gildong
	Birth date	MM DD 1990
	Gender	Male
	Employment date	MM DD 2020
Address	Sejong-daero, Jongno-gu, Seoul, Republic of Korea …	

➔ The face picture registered in the HR system for simply reading/storing purpose is general personal information.

Use the identical picture for authentication and identification purpose.

Facial recognition system



Create with certain technical means.

Original information

Feature information

➔ If the same face picture is processed for the authentication/identification purposes, then the picture becomes original information.

➔ Both the picture from the facial recognition system (original information) and feature information are applicable to protection measures recommended in this Guideline.

4 Applications

This Guideline targets personal information controller directly processing biometric information, manufacturers making biometric information processing devices and service developers/providers ("manufacturers"), and a subject ("user") using the biometric information processing service.

- Personal information controller: Public institutions, corporations, organizations, and individuals who process personal information on their own or through a different entity to operate personal information file for business
  - ※ **Personal information controllers include telecommunications service provider defined in Article 2 of the ACT ON INFORMATION AND COMMUNICATIONS NETWORK.**
  - ※ **In the case of installing and operating fingerprint recognition door lock and others privately (besides business purpose), the entity isn't considered a personal information controller.**
- Manufacturer: Corporations either making biometric information processing devices or developing a processing system and service to provide it to a customer (personal information controller, etc.)
  - ※ **This includes a manufacturer making an access control device with processing biometric information, company developing and supplying a biometric information processing system, smartphone manufacturer and OS provider processing biometric information, business operator receiving the verified value processed in a device, etc.**
- User: The subject of using biometric information processing services including access control, smartphone, application login, and transaction approval by providing biometric information
  - ※ **This includes employees and visitors using access control and service management systems, and users using a smartphone and shopping and financial applications that use biometric information.**

5 Relation to Law

- Bio information is personal information, so the PERSONAL INFORMATION PROTECTION ACT, ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT, related notice, and others are applied.
- If a special regulation is prescribed in other laws, the applicable law is applied.
  - ※ **If regulations related to bio information protection are established and amended, then the applicable regulations take precedence over this Guideline.**

Characteristics and Protection Principles of Biometric Information

1 Biometric Information Characteristics

Biometric information has uniqueness and immutability properties. When it is leaked, it is difficult to recover from the damage, and sensitive information can be misused by being extracted or forged. Thus, a special protection measure is required.

A. Uniqueness/Immutability

- Exclusively, biometric information can identify a person with itself. Once it is leaked, the damage cannot be easily recoverable due to its immutability.

→ Thus, consider **(review proportionality)** whether the risk of personal information infringement isn't greater than the benefits resulting from the introduction of biometric information application service before deciding to introduce it.

→ When introducing a service utilizing biometric information, it is necessary to **legally** collect the minimum volume of information required to be used for the service.

B. Possibility of Extracting Sensitive Information

- Sensitive information can be extracted from original information regardless of the authentication/identification purpose including race and health.

  ※ **Sensitive information including race and health is extractable from information on the face, vein, and iris.**

→ Biometric information shall be used only within **the scope of purpose** agreed by users, including authentication and identification.

→ The details on how biometric information is processed shall be **transparently** disclosed to users.

C. Possibility of Forgery

- Hacking cases with the use of biometric information extracted from silicone fingerprints and captured face and iris pictures continuously occur.

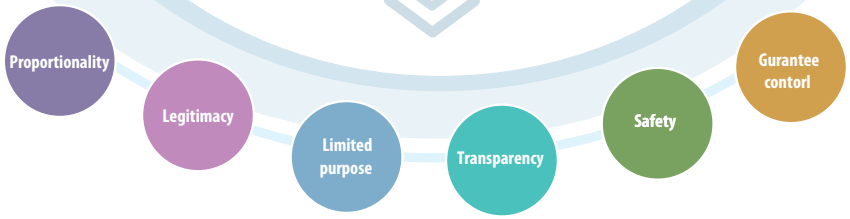
→ Biometric information shall be **safely** processed by detecting the forged biometric information registered and refusing use of the applicable service.

→ It is necessary to provide users with a means by which they can **control** biometric information on their own.

4 Protection Principles of Biometric Information

Based on Article 3 of the Principles for Protecting Personal Information of PERSONAL INFORMATION PROTECITON ACT, the top six protection principles are established by applying the characteristics of biometric information and the principle of Privacy by Design (PbD).

Principles for Protecting Personal Information of the PERSONAL INFORMATION PROTECITON ACT	Properties of biometric information	PbD
① Shall collect personal information to the minimum extent necessary and specify explicitly the purposes for which personal information is processed. ② shall process personal information in an appropriate manner necessary for the purposes and not use it beyond such purposes. ③ Shall ensure personal information is accurate, complete, and up to date to the extent necessary in relation to the purposes for which the personal information is processed ④ Shall manage personal information safely, taking into account the possibility of infringement on the data subject's rights. ⑤ Shall make public its privacy policy and guarantee the data subject's rights ⑥ Shall process personal information in a manner to minimize the possibility of infringing the privacy of a data subject. ⑦ Principle of anonymized and pseudonymised processing ⑧ Shall endeavor to observe responsibilities and obtain trust of personal information controllers.	① Uniqueness ② Immutability ③ Possibility of extracting sensitive information ④ Possibility of forgery	① Conduct prevention, emphasizing it over follow-up measures. ② Take privacy protection measures from the initial setting. ③ Create design including privacy protection. ④ Maintain balance between privacy protection and business function. ⑤ Protect the entire life cycle of personal information. ⑥ Maintain transparency in the personal information process. ⑦ Respect user's privacy.



Top 6 Biometric Information Protection Principles

① **Proportionality** Determine whether to use biometric information, taking account the scale of personal information infringement risk compared to the benefits of processing it..

② **Legitimacy** The basis of processing biometric information including its use and provision shall be legal and clear.

③ **Limited purpose** Do not use biometric information for other purposes besides authentication and identification agreed by a data subject without consultation.

④ **Transparency** Publicize items related to the protection of biometric information to a data subject.

⑤ **Safety** Process and manage biometric information safely not to be lost, stolen, forged, or damaged.

⑥ **Guaranteed control** Provide a means by which a data subject can control their own biometric information.

Protection Measures for Biometric Information
(Personal Information Controller and Manufacturer)

Protection Measures for Biometric Information (All-inclusive table)

1 Planning/ Design Phase

1. Review the necessity of biometric information.
2. Apply PbD.
3. Prepare alternative means.
4. Conduct privacy impact assessment.

2 Collection Phase

5. Legally collect biometric information.
6. Prepare measures for forged biometric information.
7. Protect the transport section when collecting and registering biometric information.

3 Use/Provision Phase

8. Use personal information within the scope of the agreed purpose of use.
9. Provide means to control biometric information.
10. Process it in collection and the input terminal.

4 Storage/ Disposal Phase

11. Encode when storing biometric information.
12. Disposal of biometric information
13. Keep original information separately.

5 Regular Inspection

14. Publicize measures used for processing personal information.
15. Manage and supervise personal information handler.

1 Planning · Design Phase

- **Determine whether to introduce biometric information service by considering the proportionality principle.**
- **Apply the PbD principle from the planning phase.**
- **Prepare and provide alternative means in addition to biometric information in prepare for cases in which users don't want to provide biometric information or cannot provide it.**
- **Conduct privacy impact assessment if a large volume of biometric information is sent to a server to be processed.**

01 Review the necessity of biometric information.

Recommended · Proportionality

- Introduce the biometric information service by considering whether the risk of personal information infringement isn't greater than the level of necessity, as well as the expected benefits when the information is used.
  - **(Before introduction)** Review whether there is any other available means can achieve the process purpose by minimizing the risk of personal information infringement of users.
  - **(When the biometric information to be introduced is selected)** Select biometric information can minimize the infringement risk while achieving its purpose since biometric information's properties are varied and the suitability for each service differs.

Note Review of necessity

- If biometric information of all subscribers is sent to the server to process authenticate one's membership on a smartphone app, then the personal information infringement risk can be considered greater than the degree of its necessity.
  - To simply authenticate membership, it is recommended to use a method of receiving the result value of authenticating biometric information processed in a safe area within the smartphone of an applicable user.
- To prevent the illegal use of a ski season ticket in a ski resort by handing it to a third party, compare and review the expected economic and administrative benefits with the infringement risk before deciding to introduce a method of using biometric information as an authentication means.

02 Apply PbD.

Recome-nded | Legitimacy | Safety | Guaranted control

- Analyze risk factors of the expected personal information infringement and take preventive measures throughout the entire phase of the biometric information service by applying the PbD* principle from the planning and design phase.

* PbD: It means applying the principle taking account the user's privacy throughout the entire life cycle of personal information process from the planning phase in developing a product and service. It is a common personal information protection principle that is used globally.

Note Measures of applying PbD principle

■ **Review items related to the entire biometric information protection service by consecutively conducting risk and infringement factor analysis and preparing alternative means in processing biometric information in the following ways: ▲analyze types and characteristics of biometric information required in applying the PbD principle, ▲determine legal grounds (consent, allowed in ordinance, etc.) in collection and use of biometric information and application methods (whether to process within a device), and ▲review the flow of processing biometric information in advance.**

Preemptive measures in the planning/design phase

- **Review legal grounds in collection and use of biometric information by analyzing types and characteristics of the information to use, and create a "flow chart of biometric information" in advance.**
  - (For identification service using fingerprints) Create the flow chart to analyze risks in advance from the prior review (consent or allowed in ordinance) of legal grounds based on collection/use, registration of fingerprints, authentication process, storage, and disposal.
- **Set the default value for product and service in a way by which user's biometric information is protected.**
  - When creating feature information, set original information to be deleted by default, etc.
- **Design an algorithm for creating feature information so that original information cannot be easily recovered from feature information. This minimizes the risk of leaks and forgery of biometric information.**
- **Prepare operation guidelines and training procedure to enable the personal information handler (operator) to safely process biometric information while running the service.**
- **When introducing existing commercial products to provide biometric information service, personal information controllers shall check whether the product safely protects biometric information before introducing it.**

Tip **To analyze risks in advance, inspect safety, and interpret regulations in applying the PbD principle. It is possible to ask advice from an external expert or specialized agency (Korea Internet & Security Agency (KISA) 118 Helpline Team, Tel: 118).**

03 Prepare alternative means.

Recome-nded | Guaranted control

- Prepare alternative means in preparation for a situation where the user doesn't want to provide or isn't capable of providing biometric information.
  * Cases: Fingerprints are damaged due to one's job, face cannot be recognized due to injury, etc.
  - Provide alternative means including an access card or password (PW) or prepare a procedure of checking identification via the face when the information is used for physical security purposes including access control and management, etc.
  - In case of an application providing information communications service, knowledge-based or ownership-based alternative means including PIN number, ARS authentication, and temporary PW are simultaneously available so that either of the methods can be chosen by the user.

Note | Alternative means (i.e.)

- Provide an access card with an IC card feature.
- Access by entering employee identification number and PW, etc. with a keypad.
- Allow access after checking one's identification card by meeting a person face-to-face (If necessary, make a person write down names in the list.).
- Operate a gate where a facial recognition camera isn't installed for a facial recognition.
- Authenticate with ID/PW and digital certificate.
- ID card for mobile devices can be used in a smartphone.

Note | Cases of supporting alternative means

- Provide an access card with an IC card feature.
- Access by entering employee identification number and PW, etc. with a keypad.
- Allow access after checking one's identification card by meeting a person face-to-face (If necessary, make a person write down names in the list.).
- Operate a gate where a facial recognition camera isn't installed for a facial recognition.
- Authenticate with ID/PW and digital certificate.
- ID card for mobile devices can be used in a smartphone.

04 Conduct privacy impact assessment.

Recommdation· duty | Legitimay | Safety

- When processing a large volume of biometric information by sending it to the server, it is recommended to conduct * privacy impact assessment.

  * **Privacy impact assessment**: In case there is a risk of an infringement with respect to personal information of data subjects due to the operation of personal information files, conduct an assessment to analyze risk factors and improve them. (Article 33 of the PERSONAL INFORMATION PROTECTION ACT)

    ※ For a public institution operating personal information files of feature information for over 50,000 users, it is required to conduct privacy impact assessment.

  - Introduce new biometric service, analyze risk factors of personal information infringement caused by major changes in the existing system, and establish protection measures by conducting privacy impact assessment.

    ※ **When processing biometric information in a central server, infringement risks including leak and misuse/abuse of biometric information are greater than when it is processed in a terminal collecting biometric information. Thus, it is necessary to analyze infringement risks and prepare improvement measures through privacy impact assessment.**

- When processing biometric information at large scale in a server, even if a handler including private business isn't subject to privacy impact assessment, it is recommended to conduct the assessment.

Related regulation

Article 33 of the PERSONAL INFORMATION PROTECTION ACT, Article 35 to 38 of the ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT, Notice of Privacy Impact Assessment , etc.

2 Collection Phase

- **Legally implement consent procedure on the collection and use of biometric information.**
- **Establish measure on the collection and use of forged biometric information.**
- **Take encryption measure not to leak or forge biometric information due to hacking when transmitting it.**

05 Legally collect biometric information.

Responsi-bility Legitimay

- When obtaining consent of collection and use of biometric information from user, shall clearly inform users on details including the collection/use purpose, collection list, and storage/use period.
- In case of feature information (sensitive information), consent on both processing of other personal information and others is required.

A. Consent Method in Collection and Use

- In agreeing with the collection and use of biometric information, shall clearly inform the following details: ① the collection/use purpose, ② collection list, ③ storage/use period, ④ a fact that a data subject has a right to refuse to agree and the details of disadvantages if there is any disadvantage due to the refusal.

Note Notice on collection and use of personal information in case of telecommunications service provider

- For telecommunications service provider, Paragraph 1 Article 39(3) of PERSONAL INFORMATION PROTECTION ACT (Special Provisions on Consent to the Collection and Use of Personal Information) is applied. Although the required notice on the consent on collection and use doesn't include **"a fact that a data subject has a right to refuse to agree and the details of disadvantages if there is any disadvantage due to the refusal,"** it is desirable to obtain consent by clearly notify the applicable details to protect user.

Comparison in notice based on Paragraph 2 Article 15 and Paragraph 1 Article 39(3)

Notice based on Paragraph 2 Article 15	Notice based on Paragraph 1 Article 39(3)
1. Collection/use purpose of personal information	1. Collection/use purpose of personal information
2. The list of personal information collected	2. The list of personal information collected
3. Storage/use period of personal information	3. Storage/use period of personal information
4. The fact on the availability of the right to refuse to agree and details of disadvantages due to the refusal	-

※For more details on special provisions on the process of personal information by telecommunications service provider and others, refer to Chapter 6 of Comment on Personal Information Protection Ordinance, Guideline, and Notice.

- For feature information, it is applicable to sensitive information according to PERSONAL INFORMATION PROTECTION ACT, *consent on the collection and use is required besides that on the processing of other personal information.

  * According to Article 23 of the PERSONAL INFORMATION PROTECTION ACT, consent on both processing of other personal information and others is required. However, when an ordinance requires or allows processing, it can be processed without consent.

- If original information is kept because of the need of personal information controllers even after the creation of feature information, shall give instruction by informing of purpose and storing period on each case when a data subject agrees to the collection and use of original information.

  ※ **The authentication and identification of biometric information are usually conducted via comparison with feature information. When feature information is created, it is mandated to immediately dispose it since the purpose for the colletion and use of the original information is achieved.**

  - The provision of service shall not be rejected for the reason that user doesn't agree with the collection of personal information besides the minimum volume of required information.
  - The collection and use consent shall be obtained as optional if it is a case where keeping original information isn't required to provide the original feature of an applicable service.

Note | **Written consent on the collection and use of biometric information (i.e.)**

Consent on the collection and use of original information			
Item	**Purpose**	**Storing/use period**	**Consent**
Face information (original information)	**[Required*]** Identify user and authenticate one's identity.	• **Until feature information to be created**	☐ Agree ☐ Disagree
	[Optional*] Study a facial recognition algorithm.	• **One year from the collection date**	☐ Agree ☐ Disagree
※ You have a right to disagree on the processing of personal information above. If you don't agree with required items, however, you cannot use the login function with your face information.			
Consent on the processing of sensitive information (feature information)			
Item	**Purpose**	**Storing/use period**	**Consent**
Face information (feature information)	Identify user and authenticate one's identity.	• **Until to leave the membership**	☐ Agree ☐ Disagree
※ You have a right to disagree on the processing of sensitive information above. If you don't agree with required items, however, you cannot use the login function with your face information.			

* Agreement to required or optional may be set differently according to the characteristics of the corresponding service.

Note Agreement method in storing original information

- In case where the use of original information collected for the authentication and identification purpose must be required to provide original function of the applicable service, it is possible to obtain all consents with other required consent at one time.
  - Using the original information collected for the authentication and identification purpose in a certain service to improve the applicable service in terms of authentication and identification is reasonably related to the original collection purpose. It is possible to predict a data subject, and there is low possibility of illegally infringe the profits of the data subject. Thus, it is possible to obtain consent along with the required consent if there is no special issue.
  - Accordingly, in case of the research and development (R&D) purpose reasonably unrelated to that of developing, improving or authenticating and identifying of other services not of the applicable service, it is impossible to obtain consent along with the required consent.
    ※ For example, when collecting audio file required in developing a voice recognition robot from AI-based service user, obtain the collection and use consent as an option.

Written consent in case of obtaining required consent (i.e.)

Consent on the collection and use of original information			
Item	**Purpose**	**Storing/use period**	**Consent**
Face information (original information)	**[Required]** • Identify user and authenticate one's identity. • **Identify this System and improve its authentication performance.**	• Until feature information to be created **or one year from the collection date**	☐ Agree ☐ Disagree
※ You have a right to disagree to the processing of personal information above. If you don't agree with required items, however, then you cannot use the login function with your face information.			

In case where the use of original information must be required to serve the original function

- Keep the minimum original audio file required in learning to improve the speaker recognition performance of the current software (v 1.0) to v 1.5 in the AI speaker.
- If an algorithm extracting a feature value to improve the facial recognition performance is changed, then keep the face image to recreate feature information with the use of the changed algorithm.

B. In Case Where There is Additional Law in Ordinance

- When ordinance requires or allows the processing of biometric information, it is possible to process it (original and feature information) without user consent.

  ※ **For the authentication and identification that uses biometric information, it is required to extract feature information. In this case, Article 15 and 23 (Limitation to Processing of Sensitive Information) of the PERSONAL INFORMATION PROTECTION ACT are applied.**

In case where an ordinance requires/allows the processing of biometric information

Ordinance	Details
Article 87(2) of ROAD TRAFFIC ACT (Verification of Identities of Persons to whom Drivers' Licenses are to be Issued)	• The commissioner of a district police agency may verify the identity of the person who intends to be issued a driver's license with the person's consent by electronically comparing their fingerprint information.
Article 7(2) of the ACT ON THE PROTECTION AND SUPPORT OF MISSING CHILDREN, ETC (Issuance, etc. of Certificate of Advance Reporting for Prompt Recovery of Missing Children, etc.)	• The Commissioner General of the Korean National Police Agency may register information on fingerprint and face of the child, etc. in the information system when a custodian of the child requests to swiftly detect the child and taking them home.
Article 8 of PASSPORT ACT (Collection, Storage, and Management of Information Necessary to Perform Passport-Related Services)	• The Minister of Foreign Affairs may collect, store, and manage information necessary to provide passport-related services, such as the fingerprint, etc.
Paragraph 10 Article 2 of ELECTRONIC FINANCIAL TRANSACTIONS ACT (Definitions)	• Biological information of users is one of the access media.
Article 24 of RESIDENT REGISTRATION ACT (Issuance, etc., of Resident Registration Certificates)	• The head of each Si/Gun/Gu shall issue a resident registration certificate to a person who has registered his/her domicile within the jurisdiction of such Si/Gun/Gu and who is at least 17 years of age; Each resident registration certificate shall contain fingerprints.
Article 12(2) of IMMIGRATION ACT (Provision of Biometrics Information at Time of Entry)	• Every alien who intends to enter the Republic of Korea shall provide their biometrics information and follow the procedures for verifying their identity.
Article 28 of IMMIGRATION ACT (Departure Inspections)	• Immigration control officials may utilize the biometrics information provided or submitted for departure inspections.
Article 14(2) of AVIATION SECURITY ACT (Checking of Identity of Passenger with Biological Information)	• Any airport operator and air transportation business entity may use biological information related administrative agency secures.
Article 19 of ADMINISTRATION AND TREATMENT OF CORRECTIONAL INSTITUTION INMATES ACT (Photographing)	• With respect to new inmates and persons transferred from other correctional facilities, the relevant warden shall have their fingerprints taken.
Article 15 of the Regulations on Prosecutory Affairs (Inquiry of Investigation Related Items)	• When a prosecutor is aware of a case, the prosecutor shall have the defendant's fingerprints taken to compare them based on the Checklist of the Criminal Record Identification System.
Article 39 of the ENFORCEMENT DECREE ON THE APPOINTMENT OF THE POLICE OFFICIALS ACT (Submission of Applications)	• Any person attempting to apply for public competitive examinations for police officials or police cadets shall submit a copy of Fingerprint Checklist.

※ **Any government and public institutions process a person's biometric information based on an applicable ordinance without user consent shall check and manage whether the information is used within the scope of the purpose allowed by the applicable ordinance.**

Note Precautions in applying Article 15 and 23 of the PERSONAL INFORMATION PROTECTION ACT

- **(Article 15)** Since biometric information is a type of personal information, when it is collected and used, it shall be applied by Article 15 of the PERSONAL INFORMATION PROTECTION ACT.
  - Thus, there may be occasions where a public institution shall observe the legal duty according to the last part of Paragraph 1(2) and Paragraph 3 to 6 Article 15 or perform applicable tasks prescribed by the ordinance, it is possible to collect and user personal information without user consent.
- **(Article 23)** However, for general authentication and identification service using biometric information, it is required to extract feature information. To process feature information (sensitive information) in the PERSONAL INFORMATION PROTECTION ACT, a public institution shall be aware that only when receiving user consent or an applicable ordinance requires or allows the processing of sensitive information based on Paragraph 1 Article 23 of the PERSONAL INFORMATION PROTECTION ACT, it is possible to process it.

Written consent in case of obtaining required consent (i.e.)

15(Collection and Use of Personal Information) ① A personal information controller may collect personal information in any of the following circumstances, and use it with the scope of the purpose of collection:

1. Where consent is obtained from a data subject;
2. Where special provisions exist in laws or it is inevitable to observe legal obligations;
3. Where it is inevitable for a public institution's performance of its duties under its jurisdiction as prescribed by statutes, etc.;
4. Where it is inevitably necessary to execute and perform a contract with a data subject;
5. Where it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party from imminent danger where the data subject or their legal representative is not in a position to express intention, or prior consent cannot be obtained due to unknown addresses, etc.;
6. Where it is necessary to attain the justifiable interest of a personal information controller, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the justifiable interest of the personal information controller and does not go beyond a reasonable scope.

23(Limitation to Processing of Sensitive Information) ① A personal information controller shall not process any information prescribed by Presidential Decree (hereinafter referred to as "sensitive information"), including ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life, and other personal information that is likely to markedly threaten the privacy of any data subject: Provided, this shall not apply in any of the following circumstances:

1. Where the personal information controller informs the data subject of the matters provided for in Article 15 (2) or 17 (2), and obtains the consent of the data subject apart from the consent to the processing of other personal information;
2. Where other statutes require or permit the processing of sensitive information.

Related regulation

Article 15, 16, 22, 23, and 39(3) of the PERSONAL INFORMATION PROTECTION ACT
Article 18 of the ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT, etc.

06 Prepare measures on forged biometric information.

Recome-nded | Safety

- When biometric information is collected and registered via devices including a sensor, prepare measures on attacks with the use of forged biometric information including silicon fingerprints, captured face and iris photos, and voice recordings.
  - **(Detection of forgery)** Apply technologies detecting forged biometric information including the application of an algorithm detecting temperature, pulse, and forgery.

Note | Technology of detecting forged biometric information (i.e.)

- Hardware method: Add hardware detecting forged biometric information by measuring the skin temperature, pulse at the top of a finger, and electric resistance flowing over the skin and by using absorbing, reflecting, permeating, and decreasing traits of light.
- Software method: Use videos collected in a sensor.
  - With the use of features where the quality of forged biometric information video is lower than that of the one collected form the actual human body, apply an algorithm analyzing the luminosity of a video, contour of the entire view, and clarity of ridge.

※ **For the application of forgery detection technology, refer to Framework on Part 1 of Biometric Type Attack Detection, KS X ISO/IEC 30107-1」 (established in Apr 2018) Korean Standards (KS), Comment on Test and Evaluation of Defense Performance on Forged Biometric Information (KISA, June 2021).**

- **(Multi-Factor Authentication (MFA))** Additionally apply knowledge- or ownership-based alternative means including PIN number, ARS authentication, and temporary PW when registering biometric information.

Note | Case of using forged biometric information

- Army surgeons made fake silicone fingerprints of the commanding officer and received overtime pay by using the fake fingerprints in a fingerprint reader for checking attendance. (Mar 2019)
- A person illegally transferred a KRW 5 billion property to one's name by obtaining required documents including the Document Certifying a Registered Seal Impression in a community center with the use of fake silicon fingerprints made by a 3D printing machine (Oct 2014).
- A German hacker group demonstrated the possibility of reproducing irises by printing out a high resolution picture of the former Russian president Putin by Googling to find the picture (Apr 2014).

07 Protect the transmission section when collecting and registering biometric information.

Responsibility Safety

- When transmitting biometric information via an information and communication network or subsidiary storage media, encrypt it with a safe algorithm to prevent leak due to unauthorized access and hacking and potential forgery.
  - Public institutions adopt an encrypted algorithm for a test object of National Intelligence Service (NIS and the private sector (corporation/group/individual) adopt the algorithm recommended by professional global institutions (KISA, National Institute of Standards and Technology (NIST), European Network of Excellence in Cryptology (ECRYPT), Cryptography Research and Evaluation Committees (CRYPTREC), etc.).

Note Safe encryption algorithm as of Dec 2018

Classification	Public institution	Private sector (corporation·group·individual)
Symmetric key algorithm	SEED, LEA, HIGHT, ARIA	SEED HIGHT ARIA-128/192/256 AES-128/192/256 Camelia-128/192/256
Public key encryption algorithm (Encryption and decryption of message)	RSAES-OAEP	RSA RSAES-OAEP, etc.
One way encryption algorithm	SHA-224/256/384/512	SHA-224/256/384/512 Whirlpool, etc.

- When processing biometric information, technical and environmental conditions differ by each institution, but each can apply a method appropriate for them among the encoding methods from common applications, SSL/TSL, and VPN.

  ※ **For encrypted algorithm methods, refer to Guideline on Encryption of Personal Information (Dec 2020) of Personal Information Protection Commission (PIPC)/KISA and the website of Active Usage of Password (https://seed.kisa.or.kr/).**

Related regulation

Paragraph 1 Article 7 of the ACT ON ACQUISITION MEASURES OF SAFETY OF PERSONAL INFORMATION,
Paragraph 3 Article 6 of the ACT ON TECHNICAL and MANAGERICAL PROTECTION MEASURE STANDARD OF PERSONAL INFORMATION, etc.

3 Use · Provision Phase

- **Use biometric information within the agreed scope of purpose from user.**
- **Provide user with means to control reading, correcting, and deleting of biometric information.**
- **If possible, process biometric information in a safe area of a terminal, collecting and registering it instead of sending and processing it in a server.**

08 Use within the agreed scope of purpose.

Responsi-bility | Limited purpose

- The biometric information obtained consent from a user for authentication or identification purposes cannot be used for other purposes, including HR management and R&D, without permission.
  - Need to manage to prevent sensitive information obtained from original information unrelated to authentication and identification purposes, including race and health conditions, from being extracted, collected, and used.
- It is required to observe legal procedures including prior consent of user for general personal information to use biometric information for other purposes besides authentication or identification.
  - In cases where a user agrees to the collection and use of personal information, inform about the purpose and storage period when using biometric information for other purposes besides authentication or identification and obtain *consent.

    * In cases where ordinance requires or allows processing, this information be processed without consent.

Note Case of using for other purposes besides authentication/identification

- Store the original picture of a face in a server taken to prove one's identification later, registered for the purpose of facial recognition.
- Use the picture registered for facial recognition to HR management, issuing of an ID card, etc.
- The function of recommending a friend's tag by identifying an individual in the picture uploaded in SNS by a user is used as both biometric and personal information.

- Even if ordinance requests or allows the processing of biometric information, it can be only used within the purpose permitted by the applicable ordinance.
  - If national or public institutions process biometric information without user consent:
    i) Clearly check the legal grounds.
    ii) Required to check and manage whether biometric information is used within the purpose permitted by the applicable ordinance through site inspection.

Note **Related overseas case where biometric information is used by a national institution**

- The European Commission (EC) presents regulations on AI, including a case where its necessity isn't applicable to certain law enforcement purposes in public places as a real-time remote biometric system. (Apr 2021)
- The Illinois senate passed a resolution greatly limiting the access of the other state or federal immigration authority to bio data of Illinois residents by considering the concern that the facial recognition technology can be unconstitutionally used based on the ground of including the execution of federal immigration laws. (Apr 2021)
- The Court of Appeal reached a verdict that the use of facial recognition technology by the police violates the human rights and information protection law in a lawsuit against automatic technology. It pinpointed that the police had too much authority and no clear guideline in using the applicable technology. (Aug 2020)
- The Democratic Party proposed a bill of Facial Recognition and Biometric Technology Moratorium Act, banning the use of facial recognition technology by federal law enforcement agencies. (Jun 2020)

Related regulation

Article 18 of the PERSONAL INFORMATION PROTECTION ACT, Article 15 of the ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT, etc.

09 Provide means to control biometric information.

Responsi-bility | Guaranted control

- Personal information controllers provide users with means, including reading, correction, and deletion, to control the provision and use of their own biometric information.
  - Support and guide users to easily use controlling functions on biometric information in devices owned by users or applications and websites provided by personal information controllers.

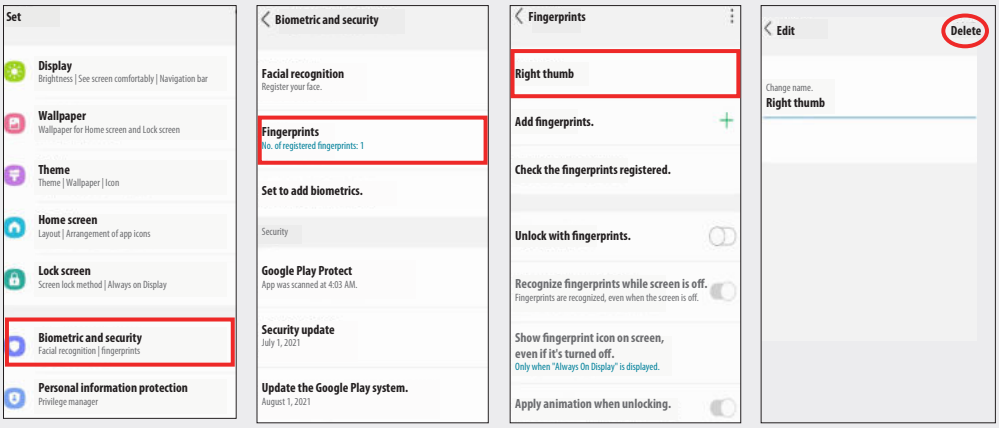
A. Control Method in Device Owned by User

- Device manufacturers or OS service providers provide users with means to correct or delete their biometric information via applicable devices or applications and websites.

Note **Example of control methods: Android phones**

① Setting → ② Biometrics and Security → ③ Fingerprints → ④ Correction · Deletion of Biometric Information

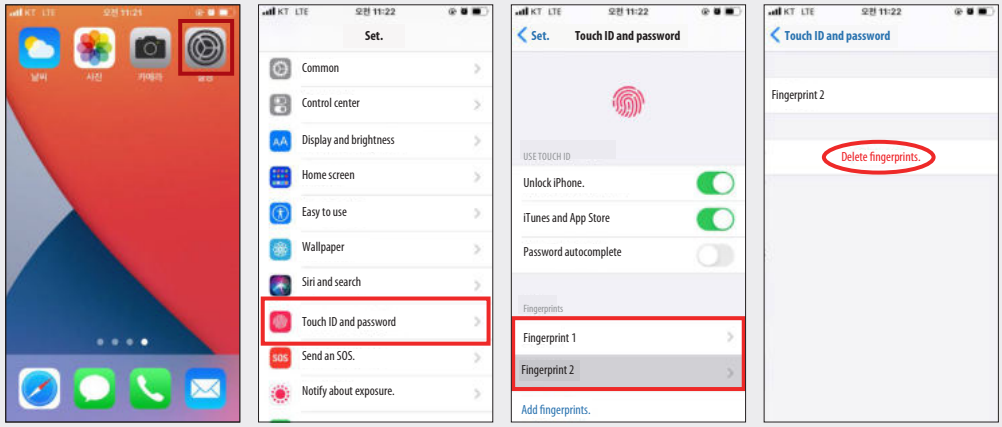
Setting method (as of Android v.11)



Note Example of control methods: iPhone

① Setting → ② Touch ID and Password → ③ Correction · Deletion of Biometric Information

Setting method (as of iOS v.14)

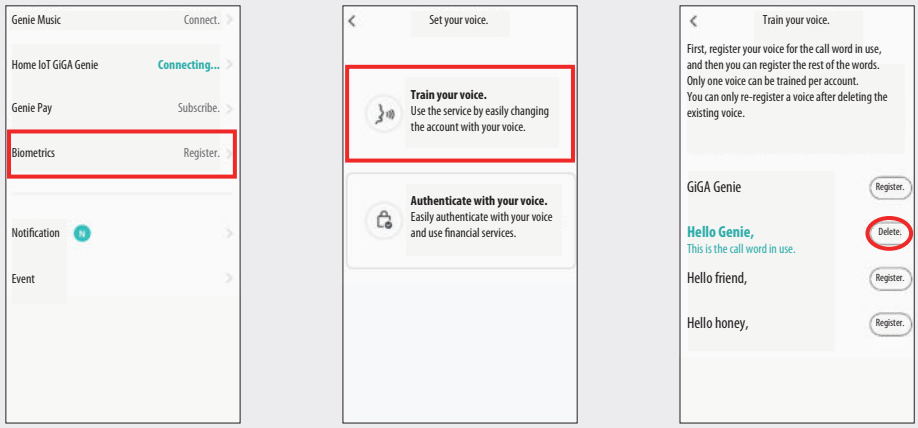


- Provide control means via websites or applications if it is difficult to directly control in devices including an AI speaker.

Note Example of control methods: GiGA Genie (AI speaker)

① Biometrics → ② Train My Voice. → ③ Correction · Deletion of Biometric Information

Setting method



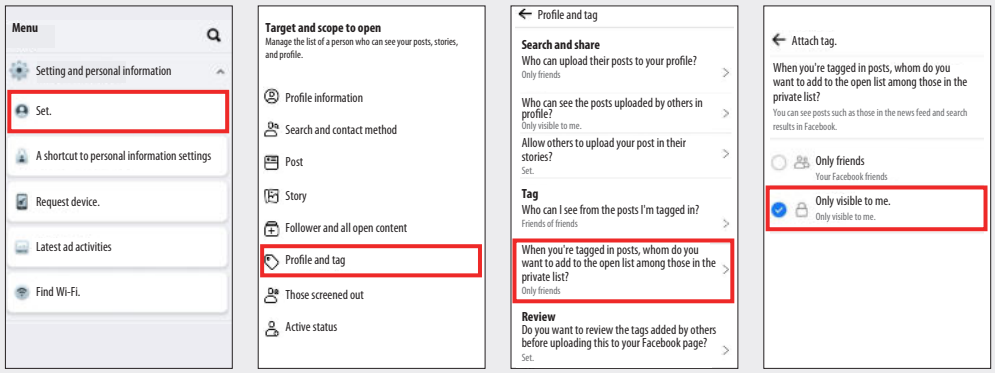
B. Control Method in Application or Website

- Provide users with means of directly controlling biometric information in applicable services if personal information controllers directly collect it or use the collected personal information, including photos and voice, as biometric information.

Note **Example of control methods: Tag recommendation feature in Facebook**

① Setting and Personal information → ② Setting → ③ Profile and Tag → ④ Change Target to Open Friend Tagging

Setting method



- In case of receiving the verified result value processed in devices including smartphones not directly collecting it, provide users with methods to control their biometric information through the cancellation menu.

Note **Guide on how to control biometric information (i.e.)**

- Biometric service ○○ self-identification service with biometric information registered in user's smartphone. We never send your information to the server and only proceed with the identification process by receiving the result value after comparing it with the biometric information registered in smartphone.
- If you want to cancel our service, please change the setting in the following menu.

Setting of service OO

Subscribe Unsubscribe

Related regulation

Article 35, 36, 37, and 39(7) of the PERSONAL INFORMATION PROTECTION ACT, etc.

10 Process biometric information in a terminal that collects and registers it.

Recommended | Safety

- When infringement occurs by transmitting biometric information to a server for processing, there is a concern that the scope of damage may increase, including the massive leak of biometric information.
  - It is necessary to first consider a way for storing and processing biometric information in a safe area within devices collecting and registering it. Media may also be directly owned by users including security tokens and smart cards.

※ **Encrypt biometric information if storing it in devices and subsidiary storage media**

Note | Safe area in devices

- Storage spaces provided by Trusted Execution Environment (TEE) and Trusted Platform Module (TPM) supported by OS.
  - Store biometric information in a safe area or store private key in the area and use it to encode biometric information. Save the encrypted information in the storage of devices and applications.

※ For Android devices, use KeyStore, TrustZone, etc. For iOS devices, it is possible to use KeyChain.

Note | Case of biometric information leak, having been stored in a server

- An Israeli security specialist detected unencrypted information including username, password, fingerprint, and facial information in the "server revealed to the internet due to an improper security setting" of a biometric information-related manufacturer. (Aug 2019)
- The DB of a U.S. federal department received an advanced persistent attack (APT) attack by a hacker group. Accordingly, personal information of 22 million former and current civil servants, along with the fingerprint information of 5.6 million of them (Jun 2015).

4 Storage · Disposal Phase

- **Encrypt biometric information with a safe algorithm when storing it.**
- **If feature information is created, then it can be considered that the original information's purpose is achieved. Thus, it shall be disposed immediately so that it cannot be recovered or replayed.**
- **When storing original information based on legal grounds or with consent from the user, store and manage the information of the applicable user separately from other users'.**

11 Encrypt biometric information when storing it.

Responsi-bility | Safety

- Encrypt biometric information (including original and feature information) with a safe algorithm to prevent infringements including forgery and leak by a third party when storing it.
  - Original information presents concern for privacy infringement in which other sensitive information including race and health can be extracted from it. It is required to use encruption to make this impossible.
  - It is required to conduct encryption since feature information can be abused for authentication and identification purpose when it is leaked.

  ※ **For encrypted algorithms, execution methods, and cases, refer to PIPC/KISA Guideline on Encryption of Personal Information (Dec 2020) and the homepage on Active Usage of Password (https://seed.kisa.or.kr/).**
- Establish and implement procedures related to the creation, use, storage, distribution, and disposal of encryption key to safely keep the encoded personal information.
  - Generate random numbers required for creating encryption keys with a safe random number generator.
  - Keep the generated keys safely so they are not revealed and, back up them in a separate device so that they are not lost due to hardware damage or software error.

Related regulation

Paragraph 2 and 5 Article 7 of the ACT ON ACQUISITION MEASURES OF SAFETY OF PERSONAL INFORMATION,
Paragraph 2 Article 6 of the ACT ON TECHNICAL and MANAGERICAL PROTECTION MEASURE STANDARD OF PERSONAL INFORMATION, etc.

12 Dispose biometric information.

Responsibility | Safety

- When biometric information is no longer required because the period of keeping and using it as agreed by the user is expired or the purpose of processing personal information is achieved, it shall be *disposed immediately.

  * Delete permanently in an irrecoverable way.

  - Usually, if feature information is created, then it means the collection and use purpose of original information are achieved. Thus, in principle, original information shall be disposed immediately.

  ※ **In cases where there are grounds in other ordinances or consent is obtained from the user, it is possible to keep and use original information.**

Note Case of keeping biometric information after its purpose is achieved

- Ski Resort A considers the vein information for the identification of customers with a season ticket as "Record on Contract or Withdrawal of Subscription which shall be maintained 5 years" based on Article 6 of the ELECTRONIC COMMERCE ACT and Article 6 of the ENFORCEMENT DECREE ON THE ACT and determines the period of storing and using vein information as 5 years.

  ➜ When the season ends, then the purpose of keeping vein information of the applicable customer is reached. Thus, it shall be disposed immediately.

Related regulation

Article 21 of the PERSONAL INFORMATION PROTECTION ACT, Article 16 of the ENFORCEMENT DECREE OF THEPERSONAL INFORMATION PROTECTION ACT, Article 13 of the ACT ON ACQUISITION MEASURES OF SAFETY OF PERSONAL INFORMATION, etc.

13 Keep original information separately.

Recommended | Safety

- If you keep the original information when creating feature information, it is recommended to keep and manage the original information of applicable user separately from other personal information to minimize damage due to its leakage.
  - Physical separation and storage should be implemented in principle. If inevitable, it is possible to logically separate it at a level equivalent to physical separation.
  - Conduct protection measures including the minimization of access to the separately kept original information, control of access, and prevention of external hacking attacks.
  - The common identifier connecting the original information of the user to other personal information uses an arbitrary value to prevent the applicable user from being directly identified.

➜ Personal information controllers including national and public institutions storing and using massive volume of personal information may be damaged greatly when original information is leaked. Thus, it is strongly recommended to apply recommendations.

Note | Recommendations for national/public institutions

- **In case of processing it based on ordinance**
  1. Clearly check the ground for processing in ordinance.
  2. Check and manage whether biometric information is used within the scope of purpose permitted by applicable ordinance via site inspection.
  3. Give clear guidance on how to collect and use biometric information through the personal information processing policy.
  4. If possible, conduct procedures for the collection and movement of biometric information, even though it is not a legal obligation.
  5. Prepare and operate systematic procedures and internal guidelines to protect biometric information.

     ※ For example, Institution A introduced global standard for records management (ISO 30301) in the fingerprint management system to enhance responsibility and transparency in the management process. (Nov 2020)
- **In case of storing and using a massive volume of original information**
  1. Keeping separately shall be applied since if the original information is leaked, the damage can be greater.
  2. Conduct biometric information protection measures recommended in this Guideline.

     ※ ① Review the necessity of biometric information; ② Apply PbD; ③ Prepare alternative means; ⑥ Prepare measures on forged biometric information; ⑩ Process biometric information in a terminal collecting and registering it.

➜ For national and public institutions processing massive volumes of original information, proactive efforts including the budgeting for the execution of protection measures above and establishment of the management system via checking and inspection are required.

5 Regular Inspection

- **Clearly provide guidance on items regarding the collection and use of biometric information via personal information processing policy, etc.**
- **Manage/supervise and train personal information handlers and trustees that directly processing biometric information.**

14 Publicize the handling policy of personal information.

Responsibility Transparency

- Clearly provide users with guidance on the use purpose, item, storage and use period, method of exerting control of user on biometric information collected and used via personal information processing policy, and enable users to check such guidance anytime.

Note Recorded responsibilities of personal information processing policy (Article 30 of Act and Article 31 of Enforcement Decree)

1. Purpose of processing personal information
2. Processing and storage period of personal information
3. Items on the provision of personal information to a third party (shall only be applied if applicable.)
4. Its disposal procedure and method (In case of maintaining it according to legal grounds prescribed in Paragraph 1 Article 21, this shall include the list of personal information to be kept along with the grounds.)
5. Items on the consignment in personal information processing (shall only be applied if applicable.)
6. Right and duty of data subject and legal representative and items on how to exert the right and duty
7. Name of the person responsible for personal information protection and the name and contact information of the department handling personal information protection and related complaints according to Article 31
8. Installation and operation of devices automatically collecting personal information including the file accessed via internet and items related to the refusal on the installation and operation (shall only be applied if applicable.)
9. List of personal information processed
10. Measures for securing safety of personal information and related items according to Article 30 or 48(2)

- Publicize personal information processing policy so that users can check easily by uploading it to a website.

※ **In case where it is not possible to upload to a website, upload to a place that can be easily seen, including a personal information handler's office, and continue publishing in publications, newsletters, promotional brochure, and bills issued more than twice a year, or include in a contract so that it can be released to users.**

Related regulation

Article 30 of the PERSONAL INFORMATION PROTECTION ACT, Article 31 of the ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT, etc.

Refer to Guideline on Writing Privacy Policy for the method for drafting the personal information processing policy and the example.

15 Manage and supervise personal information handlers.

Responsibility Transparency Safety

- Conduct management and supervision on personal information handlers participating in the development and operation of biometric application service and regular training for them.
  - Personal information controllers shall appoint a person responsible for personal information protection and conduct proper management and supervision on *personal information handlers including employees, agency workers, and part-time workers so that biometric information can be safely processed.
    * In case of using biometric information for the purpose of controlling access, etc., a working-level person at the security department conducting the registration and deletion of biometric information is also considered a personal information handler.
  - Conduct regular training for personal information handlers that directly deal with personal information to ensure they process it safely.

Related regulation

Article 28 of the PERSONAL INFORMATION PROTECTION ACT, Article 32 of the ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT, Article 15 of Standard Personal Information Protection Guideline, etc.

Establishment of Safe Usage Environment (Role of Manufacturer)

The role of the manufacturer is important to establish an environment where a person collecting and using biometric information of users, including personal information controllers, can use it safely.

1 Importance of the role of manufacturer

- Personal information controllers have a responsibility and duty to safely process biometric information according to the personal information protection ordinance.
  - Technical and administrative protection measures for safe management of biometric information are generally greatly affected by the system development and function setting of a manufacturer. Thus, the role of a manufacturer is important so that personal information controllers safely process biometric information.
- In the planning, design, and development phase of a product and service, the manufacturer applies Technical and administrative protection measures required in securing the safety of biometric information, including the encryption during transmitting and saving and safe disposal.
- For personal information handlers and individuals operating the product and service, the manufacturer provides necessary functions and use methods in safely managing and operating the biometric information processing system.

2 evelopment of safe product/service

- Apply the PbD principle from the planning/design phase and technical and administrative protection measures required in securing the safety of biometric information suggested in this Guideline to the product and service.
  - Develop globally competitive, and safe products and services by referring to *related global standards on biometric information protection.

    * Refer to Information security, cybersecurity and privacy protection - Biometric information protection, ISO/IEC 24745:2011」 (Jun 2021), Framework on Part 1 of Biometric Type Attack Detection, KS X ISO/IEC 30107-1(Apr 2018), etc.

- **(Manufacturer of making devices collecting biometric information)** In case of manufacturing devices extracting feature information by directly extracting biometric information from user via a finger scanning sensor:
  - Design an algorithm for creating feature information by making it so that the original information cannot be easily recovered to minimize risks of leakage and forgery of biometric information.

> **Related content** III. Biometric Information Protection Measure, ② Apply PbD.

  - Prepare measures in response to an attack with forged biometric information including fake silicon fingerprints, captured face and iris photos, and voice recordings when collecting original information.

> **Related content** III. Biometric Information Protection Measure, ⑥ Prepare measures on forged biometric information.

  - Once feature information is created, it shall be immediately disposed to prevent the infringement risk of personal information due to leakage unless there is any special request from the customer.

> **Related content** III. Biometric Information Protection Measure, ⑫ Dispose biometric information.

- **(Biometric information processing system/service manufacturer)** In case of online service developers, including shopping and finance applications, or information processing system manufacturers providing a certain service by verifying a user with biometric information gained from access control/attendance management system:
  - They shall encode biometric information with a safe algorithm to prevent the leak and forgery in the transmitting and storing process and safely manage encryption key.

> **Related content** III. Biometric Information Protection Measure, ⑦ Protect transmission section when collecting/registering biometric information, ⑪ Encrypt biometric information when storing it.

  - In principle, if feature information is created, the original information shall be immediately disposed. In case of storing original information due to the consent of user or legal grounds, conduct design and manufacturing so that it is kept separately from other information.

> **Related content** III. Biometric Information Protection Measure, ⑬ Keep original information separately.

- For online services, including shopping/finance applications, provide users with a means to read, correct, and delete biometric information on their own, along with the provision of biometric information.

Related content III. Biometric Information Protection Measure, ⑨ Provide means to control biometric information.

- Support functions required in technical/administrative protection measures including access authority management, access control, and access record management, generally required in the personal information processing system.

  ※ **Refer to Personal Information Protection Guideline for Developer (PIPC, Dec 2020).**

- Recommend to conduct security enhancement measures including the application of software development security (secure coding)* and inspection** on security vulnerability to prevent biometric information from being leaked, forged, and damaged, in addition to the content introduced in this Guideline.

  * Refer to Guideline of Secure Software Development (Ministry of the Interior and Safety (MOIS), Nov 2019).

  ** Refer to Security Vulnerability Inspection Guidelines (MOIS, Jun 2019), Technical/Administrative Guideline for Biometric Information Protection KS X 1966:2018 (Apr 2018), etc.

3 Instructions related to personal information handlers

- Guide personal information controllers on how to manage and operate the product and service to safely process biometric information through a product installation manual, user manual, and training.

  ※ **It is necessary to give instruction to general users (not personal information controllers) who don't use biometric information, including a fingerprint-based door lock installed at a front gate for a business.**

Note **Major instructions**

- Initial setting method including safe creation of keys when introducing devices.
- Deletion of biometric information and safe data backup method when a goal is achieved.
- Provide customers with guidance on the necessity for their consent to the collection and use of their biometric information in cases where customers are personal information handlers.
- Guide on how to safely dispose biometric information stored in devices when disposing the devices.

Guideline on Biometric Information Use (User)

Guide users on items they should be aware of before using the biometric information service for prior check, as well as specific use methods and precautions to safely use the service.

1 Prior check

1 Check whether user can control biometric information on their own.

- Check whether users can store their own biometric information in media storage for processing it, and that it is directly owned by them in forms on their smartphones, as security tokens, or as smart cards before using the service.
  - There is concern that damage can become greater due to a large=scale biometric information leak when an infringement accident occurs on a service transmitting the information to a server.
  - It is required to be careful when using the service by closely reviewing the personal information processing policy and use agreement and actively exerting control authority over the information instead of owning it by oneself to control.

2 Request proper alternative means.

- When users don't want to provide biometric information or it is difficult for them to present specific information, they cannot get service benefits. In such case, they can request other information or proper alternative means.
  - In case of physical security service including access control and attendance management, users can request alternative means, including access card and password, or procedures can be prepared to check identification face to face.
  - In case of an application providing telecommunications service, users select alternative means besides biometric service, including entering a PIN number supported by the service provider, ARS authentication, and temporary password authentication.

Related content III. Biometric Information Protection Measure, ③ Prepare alternative means.

3 Check whether the collection and use consent are obtained legally.

Check whether personal information controllers obtain the collection/use consent on biometric information legally.

- Check whether the handlers don't require the excessive collection/use consent besides the minimum required amount of information to provide their services.
- Check items to agree to be collected for specialized additional service before clicking the Consent to all items on biometric information collection/use before deciding to agree with the consent.
- It is necessary to check and obtain consent on the storing purpose and period on original information when it isn't disposed, even after feature information is created.

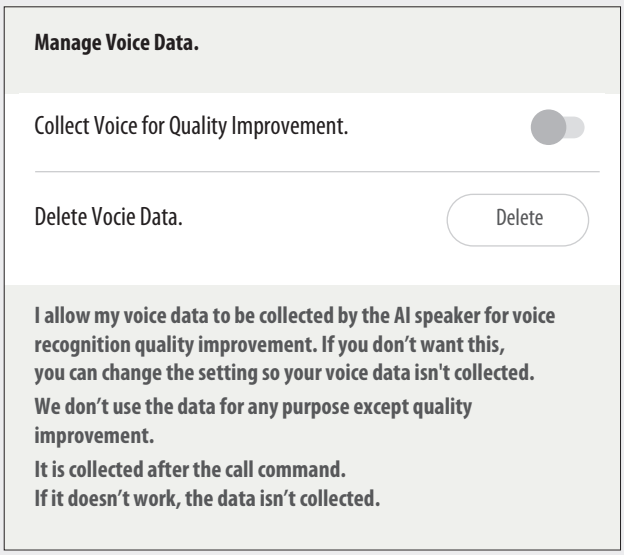
Related content III. Biometric Information Protection Measure, ⑤ Legally collect biometric information.

Check whether the service in use requests storing the original information on the server.

- Original information can be used to identify a person on its own. Once it is leaked due to its immutability trait, it is difficult to recover from the damage.
- If it isn't required in achieving the purpose of using the applicable service, it is recommended not to save the original information in the server.

Note **Consent setting on collection/use of original information**

- Company A, which provides an AI speaker service, provides a consent function on the collection of voice information (original information) for quality improvement of voice recognition. If users don't want the service, they can change the setting so that voice information isn't collected.



4 Closely review personal information processing policy and use agreement.

- Closely review the use purpose, item, storage and use period, and method of executing control by the user in regard to biometric information collected and used by service providers through the personal information processing policy and use agreement when subscribing to the service.

> **Related content** III. Biometric Information Protection Measure, ⑭ Make public of personal information processing policy.

  - Review whether there is any part where someone's personal information, including biometric information, is excessively collected or wrongfully used.
  - If original information isn't disposed after the creation of feature information, then users shall check its purpose and storage period.

2 User service

5 Check whether biometric information used for the agreed purpose.

- Check how one's biometric information is being processed and whether it is used for the purpose agreed initially by accessing the service website and application.
  - If there is concern for the infringement on rights including a case where one's biometric information is used for other purposes to which the user has not agreed, personal information controllers have a right to request the reading, stop processing, correction, and deletion of their own information.
  - Users, whose right or profit is infringed in relation to the processing of biometric information, can report the infringement to the 118 Helpline Team.

Note How to use 118 Helpline Team in KISA

- Tel: 118
- Email: privacyclean@kisa.or.kr
- Website: 118 Helpline Team (https://privacy.kisa.or.kr)

6 Exert control authority over one's biometric information.

- Check the method for controlling biometric information in one's own devices and correct or delete it if necessary.
  - Support checking on the storage of one's biometric information, deletion, and consent withdrawal functions to provide users with self-control in online services that use that information.
  - By using the applicable functions, users actively exert the right to protect their own biometric information.

Related content III. Biometric Information Protection Measure, ⑨ Provide means to control biometric information.

7 Apply additional authentication means besides biometric information.

- The biometric information, including fingerprints and face pictures stored in a smartphone, can be used conveniently in identification, transaction approval, etc., but it can also be abused by a third party without notice.
  - In case of important services including financial transaction, use additional knowledge/ownership based authentication means including PIN number, ARS authentication, and temporary password authentication.

Note Case of illegally using biometric information

- A geriatric caregiver assigned to a home sneakily downloaded the ○○ Pay application in the patient's smartphone, connected it to their account, and illegally extorted the patient's money. The caregiver approached the completely paralyzed patient in an attempt to take a photo to pass identification process requested by the app.
- A 12-year boy was tricked by a chat leader, saying "if you capture your balance in your ○○ Pay, I will give you 10 times that balance." He woke up his mother in 3:00 a.m., scanned her face with a smartphone, and withdrew the balance from her account.

VI Guideline on Application

1. In cases when directly deploying and operating service and system processing biometric information, this Guideline can be use for the following:
   - Inspect measures required in biometric information protection in planning/design phase.
   - Implementation of measures for deployment/operation phase to see whether it is safely processed.
2. If personal information controllers introduce a commercial product using biometric information, then users can use this Guideline as an inspection standard to select a product safely protect their information.
3. Manufacturers processing biometric information can use this Guideline as a design guideline and test standard in developing a product and service. This Guideline can also be used as a textbook for training developers, etc.
4. Biometric information service users can use this Guideline as an inspection standard to see whether their biometric information is safely and legally collected and used.
5. The specific execution methods of required and recommended items suggested in this Guideline can differ according to the type and method for processing biometric information. Thus, use this Guideline by comprehensively referring to the regulations of the related ordinance/notice* and Comment on Guideline/Notice and Ordinance on Personal Information Protection (Dec 2020).
   * Refer to acts, enforcement decrees, and notices related to personal information protection: Korea Law Information Center (law.go.kr).
6. Protection measures suggested in this Guideline are a minimum standard and can be observed autonomously when processing biometric information. It is recommended to prepare additional protection or new measures upon technological development.
7. For items on consultation related to this Guideline and inquiry on personal information protection ordinance, ask the 118 Helpline Team (privacy.kisa.or.kr, Tel: 118).
8. This Guideline is expected to be continuously revised and improved by applying establishment/revision of biometric information protection related ordinance/notice/policy and changes in technological environment.

※If legal regulations related to bio information protection are established and revised, then the applicable regulation precedes this Guideline.

Appendix

Appendix 1 **Self-checklist** (Personal Information Controller and Manufacturer)

Phase	Item	Checklist	[YES / NO /N/A]
Planning· Design	Review necessity.	Did you decide to introduce the biometric information service by considering whether the size of necessity and expected benefits are greater than the infringement risk? • Need to review whether there are other means besides biometric information to process the information while minimizing the infringement risk.	☐☐☐ 1-❶
	Apply PbD.	Did you analyze expected infringement risk factors in the processing phase by applying the PbD principle from the planning/design phase and take prevention measures?	☐☐☐ 1-❷
	Design/ manage algorithm.	Did you design an algorithm creating feature information by making original information cannot be easily recoverable and manage the algorithm not to be revealed?	☐☐☐ 1-❷
	Set default value.	Is the default value designed to be set as the value where users' biometric information are protected? • For example, when creating feature information, the original bio information is set to be deleted.	☐☐☐ 1-❷
	Introduce ready-made product.	In case of introducing a commercial and ready-made product to provide biometric information service, did you check whether the product safely protects the information? • This self-checklist can be used as an inspection standard to review whether the product safely protects biometric information.	☐☐☐ 1-❷
	Prepare alternative meanas.	Did you consider providing alternative means besides biometric information for authentication and identification? • In preparation for a case where users don't want to provide their information or cannot provide it due to physical challenges, etc., it is recommended to prepare alternative means, such as an access card or password.	☐☐☐ 1-❸
	Conduct privacy impact assessment.	Did you review the execution of privacy impact assessment when transmitting massive volume of biometric information to a server for processing? • If the information is transmitted to a server,then it is recommended to conduct privacy impact assessment because the infringement risk is large due to the leak and misuse/abuse instead of processing the information in a terminal that collects/registers the information.	☐☐☐ 1-❹

Phase	Item	Checklist	[YES / NO /N/A]
Collection	Legally collect biometric information.	Do you legally obtain the consent in collection/use of biometric information (original and feature information)? • Feature information (sensitive information) shall obtain consent separate from that for other personal information. ※If ordinance requests or allows the processing of sensitive information, then it is possible to process biometric information without user consent.	☐☐☐ 2-❺
	Agree to storing original information.	In case of keeping original information, rather than disposing it, when creating feature information, do you provide separate guidance about the purpose and storage period for the consent to collection/use of original information? ※In case of keeping original information according to other ordinance, then follow the applicable ordinance.	☐☐☐ 2-❺
	Prepare measures on forgery.	Did you prepare measures in regard to forged biometric information when it is collected and registered through devices including a sensor? • If forged biometric information, including fake silicon fingerprints, is collected and registered, take measure to detect this so that use of the service is rejected. • In case of registering biometric information, apply knowledge-based or ownership-based additional authentication means including PIN number, ARS authentication, and temporary PW.	☐☐☐ 2-❻
	Protect transmission section.	Did you encrypt biometric information with a safe algorithm in case of transmitting it to an information and communication network or via subsidiary storage media?	☐☐☐ 2-❼
Use/ Provision	Use within the scope of purpose agreed.	Are you using the collected biometric information within the scope of purpose, authentication or identification, as agreed by the user? • In case of using it for other purposes besides authentication/identification, you shall inform users about the use purpose and storage period as general personal information and obtain consent.	☐☐☐ 3-❽
	Provide means to control.	Is a means of control provided to users to enable them to correct or delete biometric information? • Support the correction, deletion, and cancellation of consent functions in devices owned by users or applications and websites provided by personal information controllers.	☐☐☐ 3-❾
	Process in a terminal collecting/ registering the information.	Did you consider methods for storing and processing biometric information in a safe area in devices or media that can be directly owned by a user, including security tokens and smart cards?	☐☐☐ 3-❿

Phase	Item	Checklist	[YES / NO /N/A]
Storage/ disposal phase	Encrypt biometric information when storing it.	Did you encrypt biometric information (original and feature information) with a safe algorithm when saving it?	☐☐☐ 4-⓫
	Dispose biometric information.	Once the agreed storage/usage period expires or processing purpose is achieved, do you immediately dispose biometric information?	☐☐☐ 4-⓬
	Dispose original information when feature information is created.	Do you immediately dispose original information when creating feature information • In principle, you shall dispose original information immediately when creating feature information in cases where there is no special need to keep it or no ground in ordinance.	☐☐☐ 4-⓬
	Keep original information separately.	Do you separately store/manage original information with other personal information in case of keeping it after the creation of feature information? • In case of keeping original information, it is recommended to physically or logically separate it with other personal information of the applicable user.	☐☐☐ 4-⓭
Regular inspection	Publicize personal information processing policy.	Do you provide users with contents of processing biometric information through personal information processing policy? • Publicize the policy so that users can check easily by uploading it in a website. • If it is incapable of uploading it in a website, upload in a place can be easily seen including a personal information handler's office, keep publishing in publications, newsletters, promotional brochure, and bills issued more than twice a year, or include in a contract so that it can be released to users.	☐☐☐ 5-⓮
	Manage/ supervise personal information handlers.	Do you manage/supervise personal information handlers and train them regularly?	☐☐☐ 5-⓯

Appendix 2 **Self-checklist** (User)

Phase	Item	Checklist	[YES / NO /N/A]
Prior check	Check the possibility of controlling.	Did you check whether the service is storing/processing biometric information in one's own smartphone or media can be directly owned by users including security token and a smart card? • It requires precaution in using the service since the method of processing biometric information in a server has a high risk of personal information infringement.	☐☐☐ 1-❶
	Request alternative means.	Did you request alternative means when users don't want to provide biometric information or when certain information is requested, cannot be provided them? • Alternative means supporting other biometric information including access card and password or face-to-face identification procedures can be requested.	☐☐☐ 1-❷
	Agree to legal collection/use.	Did you check whether personal information controllers are legally obtaining the collection/use consent? • Check required notification item, separate consent on feature information, etc.	☐☐☐ 1-❸
	Be careful for the consent on the collection/ use of original information.	If it is a service that keeps original information on a server, did you determine whether the user can agree or not after checking whether the original information is required in providing the fundamental service feature?	☐☐☐ 1-❸
	Review personal information processing policy.	Did you closely review the use purpose, item, storage and use period, and method of executing control by the user over their collect biometric information, which is used by service providers, through the personal information processing policy and use agreement in case of subscribing to the service?	☐☐☐ 1-❹
Use of service	Use within the scope of purpose agreed.	Did you check how your biometric information is processed and used within the agreed purpose?	☐☐☐ 2-❺
	Exert control authority.	Are you aware of a function to control (correct, delete, etc.) biometric information provided by personal information handlers? • Users shall actively exert the right to protect their biometric information including deletion of unnecessary original information and cancellation of consent in its collection/use.	☐☐☐ 2-❻
	Apply additional authentication means.	In case of important services including financial transaction, did you apply additional knowledge/ownership based authentication means including PIN number, ARS authentication, and temporary password authentication? • Be prepared for the risk of abuse by a third party, such as when the party logs into the service using the fingerprints of the user who is asleep.	☐☐☐ 2-❼

Appendix 3 **Protection Measures Recommended**

If general bio information is leaked or misused/abused, then the risk of personal information infringement is very high. Since it can be used for authentication or identification purposes at any time, it is recommended to execute protection measures equivalent to those applied on biometric information.

- Protection of transmission section: Encrypt biometric information with a safe algorithm when transmitting it to an information and communication network or via subsidiary storage media.

  ※ **For telecommunications service providers, it is a duty according to Paragraph 3 and 4 Article 6 of the ACT ON TECHNICAL and MANAGERICAL PROTECTION MEASURE STANDARD OF PERSONAL INFORMATION.**

  Related content III. Biometric Information Protection Measure, ⑦ Protect transmission section when collecting/registering biometric information.

- Encryption in saving: There is a high risk of personal information infringement if it is leaked or misused/abused, shall encrypt it with a safe algorithm when saving it.

  Related content III. Biometric Information Protection Measure, ⑪ Encrypt biometric information when storing it.

- Disposal of bio information: In principle, if there is any special reason,* then a person's physical, biological, and behavioral features used in extracting feature information shall be disposed immediately after creation of feature information.

  * It is possible to be stored and used with user consent if it is required to provide service.

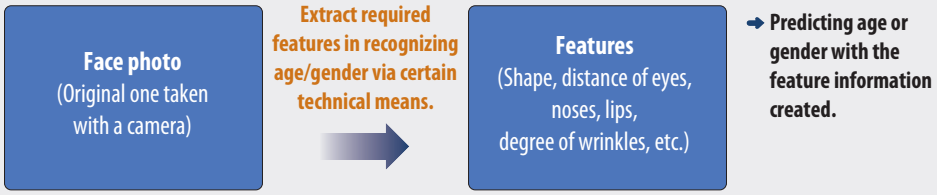
  Related content III. Biometric Information Protection Measure, ⑫ Dispose biometric information.

- Separate storage: When keeping the information on an individual's physical, biological, and behavioral features used in extracting features after features are created, it shall be stored and managed separately from other information.

  Related content III. Biometric Information Protection Measure, ⑬ Keep original information separately.

Note Case of recommending protection measures equivalent to biometric information (i.e.)

- System of sending a warning message for safe driving by determining the degree of fatigue and sleepiness of a driver with a camera installed in an autonomous vehicle (AV)
- Service releasing ads fit to a type of users by predicting their age or gender through facial recognition (photo/video)



➜ Since it is not information processed technically for authentication and identification purposes, it is applicable to general bio information.

➜ However, it is recommended to conduct protection measures equivalent to biometric information since general bio information can be always used for authentication and identification purposes.

Appendix 4 Biometric Information Protection Guideline (FAQ)

Q1 Are general photos and voice recordings stored in SNS and a cloud service, taken with a smartphone, applicable to bio information?

A If general photo and voice authenticates and identifies a person or information isn't processed through a certain technical means to identify features of a person, then the information is applicable to general personal information.

Q2 In case of a service extracting gender, age group, and emotion (lip shape) from a face photo of a user with a camera installed in a digital billboard, should the photo be encoded to save it?

A If the information to be extracted cannot be used in authenticating or identifying a person, then it is general bio information, not biometric information. Thus, it isn't necessart to encrypt it.

- However, if general bio information is leaked or misused/abused, the infringement risk is high and it can be used as authentication or identification at any time. Thus, it is recommended to conduct protecting measures equivalent to those applied on original information.

Q3 Speaker recognition goes through a process of matching the collected voice with feature information to identify registered users. In this case, does the voice of unspecified persons not users apply to the use of biometric information?

A It needs to be determined according to the process of each service. Even with this information, it may not be able to identify a certain person by being easily combined with other information. For instance, the voice of unspecified persons is immediately disposed after being matched within devices. It isn't considered personal information.

※ **If the voice of unspecified persons is sent to a server and a certain person can be identifiable, even though the information is processed only within devices, then it is biometric information. The user's consent shall be obtained for collection/use in this case.**

- However, it is necessary to clearly inform about the voice handling process so that anyone can recognize it.

Q4 I am planning to provide a service extracting information to recognize gender (male/female), age, emotions (sadness, anger, joy) from a speaker's voice. Is such information considered biometric information?

A The voice information collected only to extract gender, age, and emotion information not authenticating or identifying a person doesn't belong to biometric information but belongs to general bio information.

- Encryption, separate storage when storing original information and others are not a mandatory to general bio information.
- It is recommended to conduct protection measures equivalent to those applied to biometric information by considering the potential personal information infringement risk due to leak or misuse/abuse while applicable information is being collected, transmitted, and stored.

Q5 What is the method of consent in extracting feature information later from the previously collected personal information?

A Consent on collection/use shall be obtained in the time of necessity on both original and feature information since the use purpose differs from the previous collection/use purpose.

- In this case, the consent on feature information applicable to sensitive information shall be obtained separately from other personal information.

Q6 Can biometric information be used for other purposes besides authentication or identification purpose?

A Biometric information collected to authenticate or identify a person can be used for other purposes simultaneously.

- However, to use biometric information agreed to be used for authentication or identification purpose for other purposes, as general personal information, its collection/use purpose and storage period shall be notified. In this case, it shall be legally processed by obtaining consent.

※ **For example, the feature of recommending a friend tag by identifying a certain person in the picture uploaded in SNS by a user is a case where face information is used as both biometric and personal information.**

Q7 According to this Guideline, original information is supposed to be disposed after creating feature information. When the user extracts feature information from the photo uploaded online or into a cloud service, should the applicable photo be disposed?

A First, you need to check if personal information controllers extract feature information from the photo uploaded by the user. This might be a case of using this information for other purposes than the original purpose.

- If it is extracted with user consent, then original information may not be disposed to be used for the existing service.

Q8 When using original information with user consent, does it need to be stored and managed separately from other personal information of the applicable user?

A Enhanced protection measures are required for original information since the personal information infringement risk is very high. It is immutable; if it is leaked, it is difficult to recover the damage; and sensitive information can be leaked.

- In case of keeping original information after creating feature information by encrypting it for its safe storage, protection measures are required such as keeping it separately from other personal information.

Q9 Even if a photo already made public in SNS, etc. is used for authentication/identification purpose, do I need to encode the original and feature information to save it?

A Feature information needs to be encoded. In case of a photo (original information) made public by a user, it has no benefit of encoding it since there is no guarantee that confidentiality will be secured.

※ **Protection measures (establishment/execution of internal management plan, access control, encoding the transmission section, etc.) besides encryption need to be conducted.**

Q10 I was processing biometric information (including feature information) with user consent before the amendment in ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT (Aug 2020). Do I need to additionally obtain the collection/use consent of feature (sensitive) information from the existing user after the amendment?

A If you used feature information legally collected at the time of collection for the agreed purpose by obtaining user consent before the amendment, then you may use it without additional consent.

※ **Additional consent is needed for feature information collected after the amendment.**

Q11 Does genetic information used in a DNA test include into biometric information?

A When using genetic information* to authenticate/identify a person, it is applicable to biometric information under this Guideline.

* The term "genetic information" means information regarding the genetic features of a person, obtained by analyzing the human materials of such individual (Paragraph 14 Article 2 of BIOETHICS ACT)

- However, concerning a genetic test with genetic information, according to the BIOETHICS AND SAFETY ACT, the ACT ON USE AND PROTECTION OF DNA IDENTIFICATION INFORMATION prescribes matters on the use for investigation and prevention of a crime. Thus, the applicable law takes precedence.

Q12 What is the reason to change the term bio information to biological information?

A There is a case where bio information is considered as the information covering the entire biotechnology area. By considering that the term biological information is used in other ordinances, it has been changed to biological information.

- Moreover, you need to clearly distinguish biological and biometric information. Biometric information means information processed via certain technical means for the purpose of authenticating/identifying a certain person.

Appendix 5 **Glossary**

*in Korean alphabetical order

- **Personal information** It means any of the following information related to a living individual: (a) Information that identifies a particular individual by their full name, resident registration number, image, etc.; (b) Information which, even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual. (Paragraph 1 Article 2 of the PERSONAL INFORMATION PROTECTION ACT)

  ※ Whether or not there is ease of combination shall be determined by reasonably considering the time, cost, technology, etc. used to identify the individual, as well as the likelihood that the other information can be procured.

- **Privacy impact assessment** In the case there is a risk of an infringement with respect to personal information of data subjects due to the operation of personal information files, shall conduct an assessment to analyze risk factors and improve them. (Article 33 of the PERSONAL INFORMATION PROTECTION ACT)

- **Consignment of personal information processing task** It means personal information handlers consign the collection/use of personal information itself or a task including the collection/use to a third party (trustee).

- **Privacy by Design (PbD)** It means a principle of applying privacy and personal information protection technology and policy throughout the entire cycle from the planning to disposal phase.

  It consists of top 7 principles: ①Prevention is emphasized over follow-up measures, ② Privacy protection measure from the initial setting, ③ Design where privacy protection is considered, ④Balance between privacy protection and business function, ⑤ Protecting the entire personal information life cycle, ⑥ Maintenance of visibility and transparency in the personal information handling process, ⑦ Respect of user's privacy.

- **Personal information processing policy** It documents personal information processing standard and protection measures of personal information controllers including other matters prescribed in Article 30 of the Act. (Article 30 of the PERSONAL INFORMATION PROTECTION ACT)

- **Personal information controller** It means a public institution, legal person, organization, individual, etc. that processes personal information directly or indirectly to operate the personal information files as part of its activities. (Paragraph 5 Article 2 of the PERSONAL INFORMATION PROTECTION ACT)

- **Personal information handler** While processing personal information, a personal information controller shall conduct appropriate control and supervision against the persons who process the personal information under their command and supervision, such as an officer or employee, temporary agency worker and part-time worker to ensure the safe management of the personal information. (Paragraph 1 Article 28 of the PERSONAL INFORMATION PROTECTION ACT)

- **Personal information profile** It means a set or sets of personal information arranged or organized in a systematic manner based on a certain rule for easy search of the personal information (Paragraph 4 Article 2 of the PERSONAL INFORMATION PROTECTION ACT)

- **Sensitive information** It includes ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life, and other personal information that is likely to markedly threaten the privacy of any data subject, any information prescribed by the ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT (Paragraph 1 Article 23 of the PERSONAL INFORMATION PROTECTION ACT)

- **Biometric information** It is biological information processed through a certain technical means to authenticate/identify a certain person. It is divided into biometric original and feature information.
- **Biometric original information** It is information on biometric information collected/registered via devices to authenticate/identify a certain person.
- **Biometric feature information** It is information of biometric information created through a certain technical means of extracting features from original information. It belongs to sensitive information according to Paragraph 3 Article 8 of the ENFORCEMENT DECREE OF THE PERSONAL INFORMATION PROTECTION ACT.
- **Bio information** As information on physical, biological, and behavioral features of a person including fingerprints, face, irises, veins, voice, and handwriting, it is information processed through a certain technical means to either authenticate/identify a certain person or understand one's features (age, gender, emotion, etc.).
- **User** A data subject using services including access control, logging in smartphone/app, and transaction approval by providing one's biometric information.
- **Data subject** It means an individual who is identifiable through the information processed and is the subject of that information. (Paragraph 3 Article 2 of the PERSONAL INFORMATION PROTECTION ACT)
- **Telecommunications service provider** It means telecommunications operators and persons who supply information or relay the information supply using the telecommunications services to pursue profits. (Subparagraph 3 Paragraph 1 Article 2 of the ACT ON INFORMATION AND COMMUNICATIONS NETWORK)
- **Manufacturer** It means corporations providing customers (personal information controller, etc.) with device processing biometric information by manufacturing it or a biometric information processing system/service by developing it.

Appendix 6 **Reference**

1. Comment on Guideline/Notice and Ordinance on Personal Information Protection, PIPC. Dec 2020
2. Comment on ACT ON ACQUISITION MEASURES OF SAFETY OF PERSONAL INFORMATION, PIPC, Dec 2020
3. Comment on Technical/Administrative Protection Measure on Personal Information, PIPC, Dec 2020
4. Guideline on Encryption of Personal Information, PIPC, Dec 2020
5. Guideline on Execution of Privacy Impact Assessment, PIPC, Dec 2020
6. Guideline on Minimizing Collection of Personal Information, PIPC, Dec 2020
7. Personal Information Consignment Guideline, PIPC, Dec 2020
8. Guideline on Writing Privacy Policy, PIPC, Dec 2020
9. Guideline on Processing Online Personal Information, PIPC, Dec 2020.
10. Personal Information Protection Guideline for Developer, PIPC, Dec 2020
11. Technical/Administrative Guideline for Biometric Information Protection, KS X 1966:2018, Apr 2018
12. Framework on Part 1 of Biometric Type Attack Detection, KS X ISO/IEC 30107-1, Apr 2018
13. Information security, cybersecurity, and privacy protection - Biometric information protection, ISO/IEC 24745:2011, Jun 2011
14. Information technology - Vocabulary - Part 37: Biometrics, ISO/IEC 2382-37:2017, Feb 2017
15. Telebiometrics protection procedures - Part 1: A guideline on technical and managerial countermeasures for biometric data security, ITU-T X.1086, Nov 2008
16. Security Vulnerability Inspection Guidelines, MOIS, Jun 2019
17. Guideline of Secure Software Development, MOIS, Nov 2019
18. Comment on Test and Evaluation of Defense Performance on Forged Biometric Information, KISA, Jun 2021
19. Password Guide, Ministry of Science and ICT, Jun 2019

※ **The latest materials on comments | guidebook | policy | guideline related to personal information are uploaded in the sitemap (policy | ordinance/ legal information/ policy | guideline) of PIPC (www.pipc.go.kr) and its web portal (materials/instructional material) (www.privacy.go.kr).**

Date of publication: September 2021
Place of publication: Personal Information Protection Commission (PIPC)
Support organization: Korea Internet & Security Agency (KISA)

- This Guideline is to be continuously revised and improved based on the establishment and amendment of bio information-related ordinance and changes in the technology environment.
- You may find the latest material in the sitemap of PIPC (www.pipc.go.kr) and its web portal (www.privacy.go.kr).