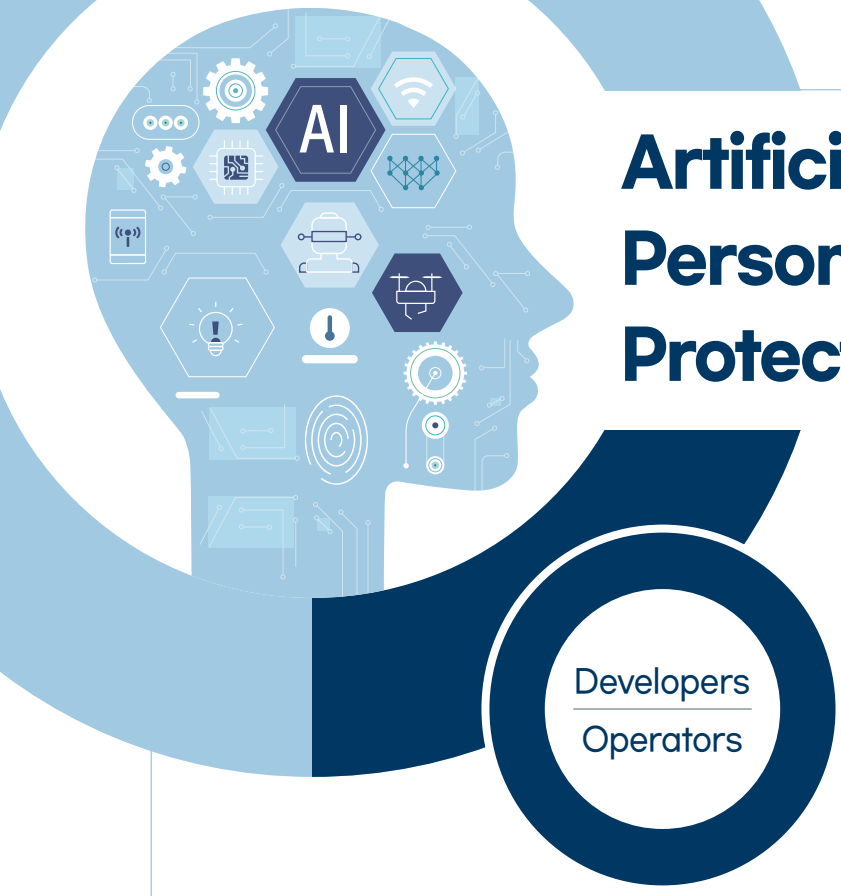


Artificial Intelligence (AI) Personal Information Protection Self-Checklist

May 31, 2021

Developers

Operators

Personal Information Protection Commission

Information

- **This self-checklist was prepared for the purpose of not only complying with the obligations regarding personal information protection, but also providing information on matters necessary for implementing and checking autonomous personal information protection suitable for its technology and service environment in consideration of the fact that AI technology and service are continuously developing and changing.**

  ※ As it includes the guidelines pursuant to the 「Personal Information Protection Act」, personal information controller in areas other than AI service can also use the checklist.

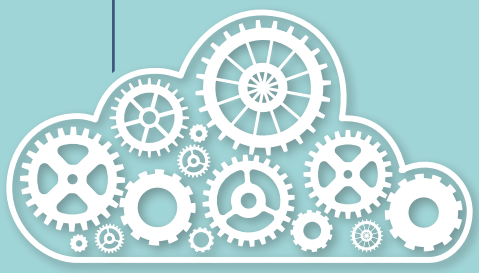
- **The specific method of implementing the obligations and recommendations included in the self-checklist may vary depending on the type and method of personal information processing, please refer to and use the related detail provisions and notifications*, the "Explanation of personal information protection laws, guidelines and notifications (December 2020)" and related materials like guideline** comprehensively.**

  * personal information protection related provisions, enforcement decrees, notification, etc.: See the Korean Law Information Center (law.go.kr).

  ** See the Personal Information Protection Commission website (www.pipc.go.kr) and the personal information protection portal (www.privacy.go.kr).

- **For consultation on the self-checklist and inquiries on personal information protection laws, please contact the 'Personal Information Infringement Report Center' (privacy.kisa.or.kr or call 118).**

CONTENTS



Outline

1. Background

- As new services that apply artificial intelligence (AI)[1] are introduced and spread in the intelligence information society, it is likely to cause various social problems such as personal information infringement.
  - When AI technology and service are developed and operated (hereinafter referred to as 'AI development and operation'), it is necessary to secure the safety and reliability of personal information processing.

- We will prepare the self-checklist, necessary for enhancing the awareness of persons participating in AI development and operation (hereinafter referred to as 'AI developers and operators') about personal information protection and autonomously protect personal information, and provide information on it.

2. Who uses it

- AI developers and operators who have the status of personal information controllers (including information and communications service providers, etc.*) and personal information handlers pursuant to the 「Personal Information Protection Act」

  * Chapter 6 of the 「Personal Information Protection Act」 stipulates the 'special cases concerning processing of personal information by providers of information and communications services or similar.' (the special provision will be applied first if they fall under the status of an information and communications service provider, etc.)

1 **Artificial intelligence (AI)**: A scientific technology that materializes human intelligence with computers, including the ability to ① recognize the situation, ② judge and act rationally and logically, and ③ perform emotional and creative functions (Source: relevant authorities, and national AI strategy (December 2019))

3. Characteristics

- **(Regular checklist)** The self-checklist that AI developers and operators can utilize during pre-inspection of guidelines or non-periodic inspection of service operations pursuant to the 「Personal Information Protection Act」 to process personal information lawfully and safely and prevent infringement

- **(Education guidebook)** The guidebook which can be used for personal information protection guideline education and consulting that persons in charge of AI technology and service should be familiar with

4. Composition

- **6 principles of AI personal information protection:** legitimacy, safety, transparency, participation, responsibility and fairness

- **AI personal information protection self-checklist:** It consists of 16 items to check concerning the legal obligations[2] to comply in stages (or regular) or recommendations[3], and 54 items to verify

- **Information on utilization:** How to use the checklist and contact points for consultation, etc.

2 **Obligations:** Items that must be complied with according to protection laws. Penalties may be imposed if they are violated (Chapter 10 of the Personal Information Protection Act).

3 **Recommendation:** Items that are not statutory obligations, but can help protect personal information and prevent infringement protection if they are complied with

Characteristics and principles of personal information processing in AI

1. Characteristics and basic direction of AI-related personal information processing

- **(Processing of large data)** A large amount of learning data is utilized during AI development, and it is highly likely that various kinds of personal information and sensitive privacy data are included in it. Also, there are high demands for continuous utilization of such data during service operation.
  - **It is important to collect personal information in a legitimate way, e.g. data subjects' consent and pseudonymization, use it within foreseeable and permitted purposes, and safely manage it.**

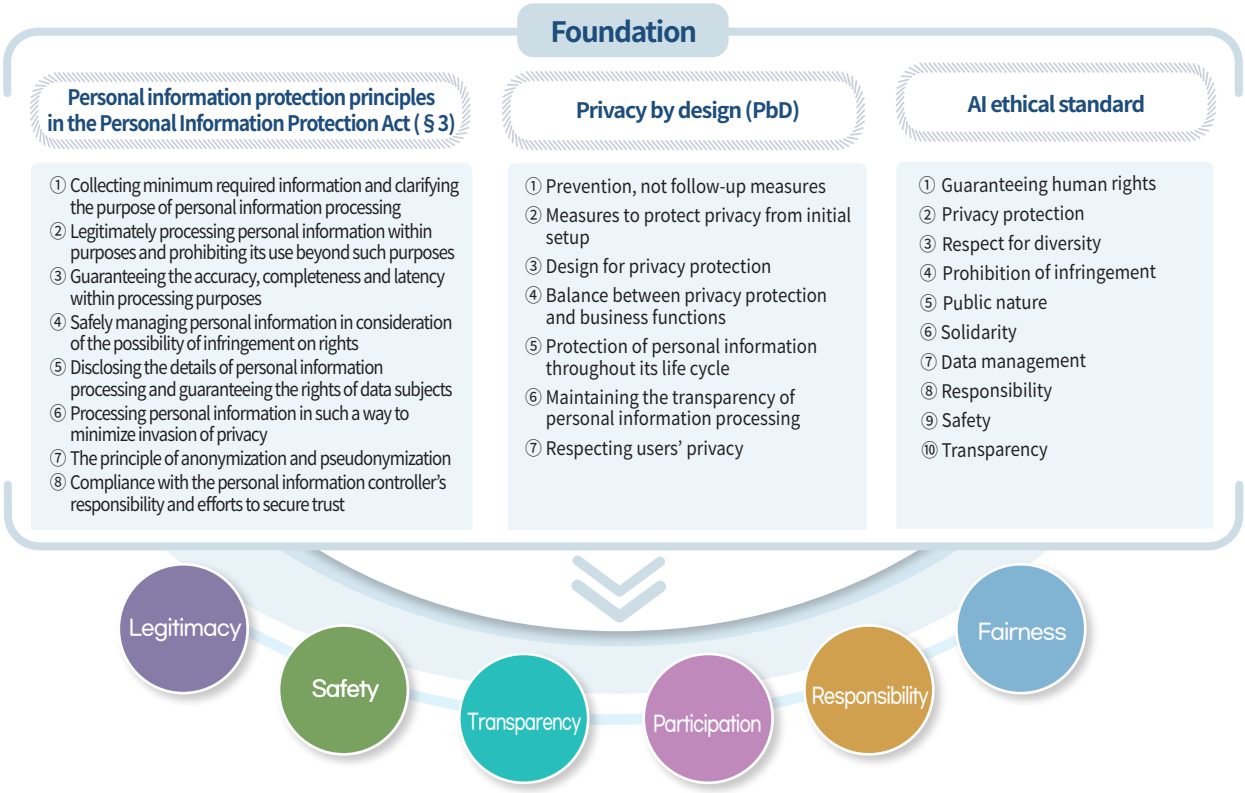
- **(Complexity and opacity)** The personal information processing method in the process of developing and operating AI service is very complicated, and as it is difficult for users to know how their personal information is processed, data subjects' exercise of rights may be limited.
  - **It is important to guarantee user participation by transparently disclosing the details of personal information processing so that data subjects can exercise their rights in regard to the processing of their personal information.**

- **(Automation and uncertainty)** In general, the AI model uses the knowledge and probability-based reasoning method to analyze and process data. As it is difficult to predict the results of data processing in the process of using it to develop and operate automated service data, such problems as privacy infringement, social discrimination and bias may arise
  - **To ensure that privacy is protected, it is important to responsibly manage personal information processing, and it is necessary to consider the fairness of the results of personal information processing so that users are not discriminated.**

2. 6 principles of AI-related personal information protection

- For personal information protection in consideration of the characteristics of personal information processing of the AI technology and service, not only compliance with the obligations pursuant to current laws, but also autonomous protection activities and responses to ethical issues are important.

- Accordingly, based on the protection principles (§3) pursuant to the 「Personal Information Protection Act」, which contains internationally accepted personal information processing principles, 6 AI-related personal information protection principles were derived by reflecting the 「Privacy by Design」 principles for autonomous protection activities, and the 「AI ethical standards」 (December 2020, Ministry of Science and ICT) for responding to ethical issues.



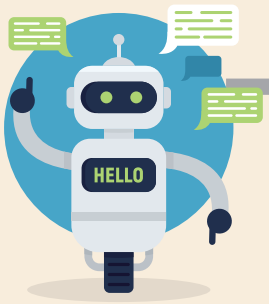
6 principles

① Legitimacy The grounds for processing, e.g. personal information collection, use and provision must be legitimate and clear.
② Safety Personal information must be processed and managed safely.
③ Transparency The details of personal information processing must be disclosed that that data subjects will easily see them.
④ Participation There must be a communication system in regard to personal information processing, and the rights of data subjects must be guaranteed.
⑤ Responsibility The responsibility for personal information processing management must be clear.
⑥ Fairness Personal information must be processed in a way suitable for the purpose of collection to minimize social discrimination and bias.

AI Personal information protection self-checklist

1. Overall flowchart

Inspection by stage



Stage 1 Planning and design

❶ Apply the **PbD principle** from the planning and design stage

❷ Conduct **personal information impact assessment**

Stage 2 Personal information collection

❸ **Implement** legitimate personal information **consent method**

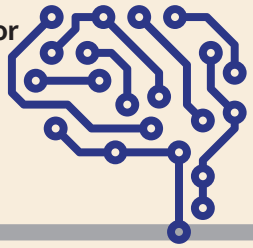
❹ **Check the grounds of personal information collection other than consent**

❺ **Notify the source of** personal information other than data subjects **and the purpose of personal information processing**

Stage 3 Personal information use and provision

❻ **Use personal information within collection purposes** and check separate grounds if personal information **is collected for purposes other than provision to a third party**

❼ If **pseudonymized information** is **processed, comply with permitted purposes and standards.**



Stage 4 Storage and destruction of personal information

❽ **Safely store and manage** personal information through measures like encryption and access control

❾ If **personal information** becomes **unnecessary, immediately destroy it.**

Regular inspection

Regular 5 AI service management and supervision

⑩ **Manage and supervise personal information handlers** and provide regular education for them.

⑪ **When personal information processing is outsourced**, document management items, and provide **education for outsourcees, manage and supervise** them.

Regular 6 Protection of AI services users and damage relief

⑫ Transparently disclose **the privacy policy.**

⑬ Prepare a procedure for **users' request to exercise the right** and implement it.

⑭ When **personal information is leaked,** prepare the procedure **for notifying it to data subjects, reporting to related agencies, and providing damage relief.**

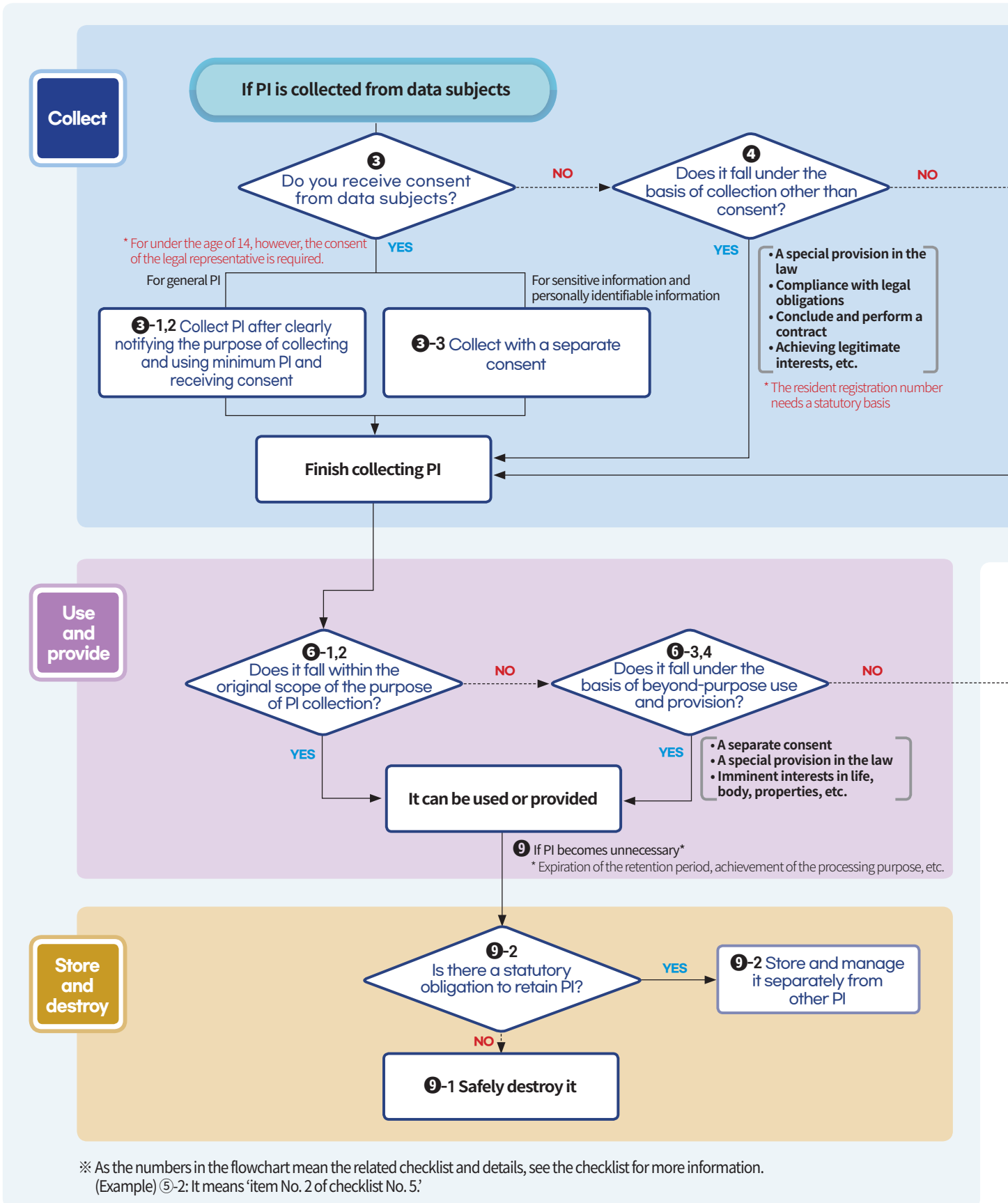
Regular 7 Autonomous personal information protection activities

⑮ Proactively carry out **autonomous protection activities.**

Regular 8 Checking AI ethics

⑯ **Constantly check and improve ethical issues.**

2. Legitimate PI* processing flowchart (* Personal Information)



※ As the numbers in the flowchart mean the related checklist and details, see the checklist for more information.
(Example) ⑤-2: It means 'item No. 2 of checklist No. 5.'

※It explains the flow and judgments to make in regard to general PI processing in an easy-to-understand way, and the order and connectivity may vary depending on the situation.

Personal information

If PI is collected from sources other than data subjects

If PI is collected from a third party

❺-2 Was the PI collected and provided based on legitimate grounds*?

NO

YES

* It is possible to use and provide PI within permitted purposes.

If public information is collected

❺-3 Is the scope reasonable in consideration of the disclosed intent*?

NO

YES

* A reasonable scope in which the data subject's will to consent is recognized, etc.

Review the grounds of processing

Review the grounds of collection

Pseudonymized information

❼-1 Does it fall under the permitted purpose of processing pseudonymized information*?

NO

YES

* Statistical purposes, scientific research, and archiving purposes in the public interest, etc.

❼-3 Safely pseudonymize

Do you combine pseudonymized information?

NO

YES

If combined within the same PI controller

If combined between different PI controllers

Safely combine pseudonymized information

❼-5 Combine pseudonymized information through a combination agency (analysis, exporting, etc.)

Use pseudonymized information

Anonymized information

Safely anonymize

※ As it is no PI, it can be utilized freely (not subject to the PI Protection Act)

3. Personal information protection self-checklist by stage

1 Planning and design

[YES / NO / N/A]

1 **From the AI technology and service planning and design stage, according to the PbD* principle, did you analyze and remove personal information infringement risks, and reflect the guidelines and privacy protection plans pursuant to the 「Personal Information Protection Act」 (hereinafter referred to as the 'Act') and the enforcement decree (hereinafter referred to as the 'enforcement decree') of the same Act in the AI development and operation plan?** Safety Responsibility Fairness

Recommended

*Privacy by Design (PbD): It means reflecting the technology and policy considering users' privacy in the design throughout the life cycle of personal information processing from the planning stage when products and services are developed, and it is a personal information protection principle that is widely used around the world.

➡ **If the adequacy of collecting personal information that will be collected and used for AI development and the privacy infringement risks of the modeling, learning and operation process are reviewed in advance and the risk factors are removed, AI service's likelihood of infringing on privacy can be lowered and safety and reliability can be increased.**

Check 1 **Did you apply the PbD principle during the planning and design of AI technology and service to analyze and remove personal information infringement risks?** (§ 3⑥ of the Act)

- Example of PbD application: Securing the safety of personal information processing by reviewing the overall flow of personal information processing in advance from the planning and design stage, and taking safety measures, such as deciding not to collect unnecessary personal information, and analyzing, removing and encrypting risks and infringement factors.

Check 2 **Did you reflect prevention of privacy infringement and reinforcement of personal information protection in the AI development and operation plan?** (§ 3⑥ and ⑧ of the Act)

- Article 3 of the Act (Principles for Protecting Personal Information) stipulates that the personal information controller should process personal information in a manner to minimize the possibility of infringing the privacy of a data subject, and endeavor to obtain trust of data subjects by observing and performing such duties and responsibilities as provided for in this Act.

Related provisions

Article 3 of the Act, PbD principle, Article 4 of the「Standard Personal Information Protection Guideline」(hereinafter referred to as the 'Standard Guideline'), etc.

Cf.

1. **To apply the PbD principle, you can "① Identify the overall data status you want to collect and use → ② Analyze personal information items and types (identifier, attribute information, etc.) → ③ Determine the grounds for collecting each personal information item (consent, etc.) and utilization methods (pseudonymization, etc.) → ④ Prepare the personal information processing flowchart" in advance, and review personal information protection-related information on services by analyzing the risks and infringement factors of personal information processing, and preparing alternatives sequentially.**
2. **You can receive advice from external experts or send inquiries to specialized institutions* for advance risk analysis, safety inspection, and interpretation of laws.**

   * Korea Internet & Security Agency (personal information infringement report center, call 118), etc.
3. **See the「automatically processed personal information protection guideline (with focus on cases of PbD application, December 2020)」.**

2 When there is a concern about the data subject's personal information infringement in the AI development and operation process, did you review and carry out impact assessment*? Safety Legitimacy

[YES / NO / N/A] ☐☐☐

Public: Mandatory

Private: Recommended

*Personal information impact assessment: Analyzing risk factors and deriving improvements when there is a concern about the data subject's personal information infringement due to operation of personal information files

➡ **As unexpected personal information infringement may occur in the process of AI technology development and operation process due to the characteristics of AI technology, it is possible to improve the safety of the AI service and system by analyzing risk factors in advance and conducting impact assessment to derive improvements.**

Check 1 **Did public institutions, obligated to conduct impact assessment, (§ 33 of the Act and § 35 of the Enforcement Decree) conduct impact assessment?** ☐☐☐

- Obligated to conduct impact assessment: In case of personal information files, managed by a public institution pursuant to Subparagraph 6 of Article 2 of the Act with "sensitive information and personally identifiable information of 50,000 or more people, system links with 500,000 or more people and personal information of 1 million or more people," or if the operating system is changed after impact assessment (§ 35 of the Enforcement Decree)

Check 2 **When there is a concern about personal information infringement due to service*, did private businesses review the necessity of personal information impact assessment even if they are not obligated to conduct impact assessment?** (§ 33⑧ of the Act) ☐☐☐

* If there is a serious change in the method of personal information processing or AI service, related to personal information, is newly developed as AI technology is applied, it is possible to lower the level of the infringement risk by conducting impact assessment and making improvements.

Related provisions

Subparagraph 6 of Article 2 and Article 33 of the Act, Articles 35 through 38 of the Enforcement Decree of the same Act, the 「Notification on the personal information impact assessment」, etc.

Cf.

■ **For more information, see the 「Guide to the Personal Information Protection Act, guidelines and notifications (December 2020)」 (hereinafter referred to as the 'guide'), the 「Guidebook for personal information impact assessment (December 2020)」, etc.**

2 Collecting personal information

3 **When consent to collection of personal information is received from data subjects to develop and operate AI, was the method of obtaining consent legitimate?** Legitimacy

[YES / NO / N/A] ☐☐☐

Mandatory

➡ **When consent to collection of personal information is obtained, personal information items to be collected, the purpose of processing personal information, the right to refuse to consent, and the details of disadvantages if there is any disadvantage to data subjects who refuse to consent must be notified specifically to them in advance, and their consent must be obtained according to the voluntary will of the data subjects.**

Check 1 **Did you minimize personal information collection items when consent to personal information collection is obtained?** (§ 16, § 22 and § 39-3③ of the Act) ☐☐☐

- Minimum personal information necessary for the purpose will be collected after obtaining mandatory and optional, and service provision should not be denied even if consent to collection of personal information other than minimum information is not obtained
- Consent to marketing and advertising: When receiving consent to personal information processing for the purpose of promotion and sale of products, data subjects must be clearly informed of this, and it must be distinguished from other consent.

Check 2 **Do you receive consent to collection of personal information in advance specifically and clearly according to the voluntary will of the data subjects?** (§ 15, § 22 and § 39-3 of the Act) ☐☐☐

- When the data subject's consent to personal information processing is received, each matter requiring consent must be distinctly presented, and the purpose of collection and use, the personal information items to be collected and used, and the collection period must be clearly notified.

[Example of application to AI] If consent to collection and use of personal information necessary for "development of new AI service" is received, the meaning of the 'new service,' the scope and purpose of using the personal information must be notified specifically for the data subject' full understanding and prediction.
If it is difficult to receive consent, you may check if you can use the personal information by checking if the scope is reasonably related to the original purpose of collecting the personal information (See Checklist ⑥), and if it is possible to achieve the purpose using pseudonymized information, you can check if it falls under the permitted scope, i.e. 'scientific research, statistical purposes, etc.' and use the personal information in compliance with established standards. (See Checklist ⑦)

<Example of receiving consent to collection and use of data for AI learning>

- Personal information collection item: The personal information items, e.g. "OO SNS dialog information," must be specified.
- Purpose of collection and use: It must be specified like "development of the chatbot algorithm of OO service (for learning)."
- Retention and use period: The personal information items will be retained and stored for development of OO algorithm for O months. However, the personal information may be pseudonymized for the purpose of scientific research, statistical purposes and preservation of records for public interest, etc. and retained and used for the minimum required period.

* You must inform the data subjects that they have the right to refuse to consent, and if there is any disadvantage when they refuse to consent, you must mention it.

- Example of a wrong consent: Including the comprehensive purpose of collecting and using personal information in the privacy policy and providing the link, and deeming the data subject to have consented even if he/she did not check the details

Check 3 **When collecting sensitive information* and personally identifiable information**, do you receive a consent separately from the consent to the processing of other personal information?** (§ 23 and § 24 of the Act) ☐☐☐

* sensitive information (§ 23 of the Act and § 18 of the Enforcement Decree): Personal information highly likely to infringe on the privacy of data subjects, e.g. ① ideology and belief, ② joining a labor union or political party and withdrawing from it, ③ political views, ④ health, ⑤ information on sex life, etc., ⑥ genetic information, ⑦ information corresponding to a criminal history, ⑧ biometrics (characteristics), ⑨ information on race or ethnicity

** Personally identifiable information (§ 24 of the Act and § 19 of the Enforcement Decree): ① passport number, ② driver's license number, ③ alien registration number, etc. If there are no specific grounds in the Resident Registration Act, the Presidential Decree or the rules of a constitutional institution, however, it cannot he processed. (§ 24- 2 of the Act)

Check 4 **When collecting the personal information of children under 14, do you receive the consent of their legal representatives?** (§ 22 and § 39-3④ of the Act) ☐☐☐

- In this case, the minimum information necessary for receiving consent from the legal representative (the name and contact information of the legal representative) can be collected from the children.

Check 5 **When notifying personal information processing items to children, do you use easy-to-understand forms and a clear and easy language?** (§ 39-3⑤ of the Act) ☐☐☐

- If notification related to personal information processing is sent to children under 14, it must be easy to understand.

Related provisions

Articles 3, 15, 16, 22, 23, 24, 39-3 of the Act, Articles 17 through 19 of the Enforcement Decree, Article 4 of the「Notification on personal information processing methods」, Articles 12 through 13 of the standard guideline, etc.

Cf.

■ **For more information, see the guidebook, the「Guideline on minimization of personal information collection (December 2020)」, the「Guideline on online personal information processing (December 2020)」, etc.**

4 When you wanted to collect personal information without receiving consent for the purpose of using it for AI development, etc., did you check the grounds permitted by law? Legitimacy

[YES / NO / N/A]

Mandatory

➡ **Clarify the basis for collection by checking whether personal information can be collected without consent, such as when it is unavoidable for the conclusion and implementation of a contract with data subjects.**

Check 1 **Does it fall under a reason for collecting personal information without the consent of the data subjects?**

Personal information controller

- Where special provisions exist in other laws or it is inevitable to observe legal obligations (§ 15①2 of the Act)
- Where it is inevitable for a public institution's performance of its duties under its jurisdiction as prescribed by statutes, etc. (§ 15①3 of the Act)
- Where it is inevitably necessary to execute and perform a contract with a data subject (§ 15①4 of the Act)
- Where it is deemed manifestly necessary for the protection of life, bodily or property interests of the data subject or third party (§ 15①5 of the Act)
- 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 (§ 15①6 of the Act)

Information and communications service providers

- Where the information is necessary in implementing a contract for provision of information and communications services, but it is clearly difficult to obtain ordinary consent for economic and technical reasons (§ 39-3②1 of the Act)
- Where the information is necessary to calculate fees for the provision of information and communications services (§ 39-3②2 of the Act)
- Where special provisions exist in other laws (§ 39-3②3 of the Act)

Check 2 **When you want to receive pseudonymized information from a third party without data subjects' consent, and collect and use it, do you comply with the "check items on Checklist ⑦"? (§ 28-2 of the Act)**

- In this case, the purpose of processing pseudonymized information must fall under the scope permitted by law, e.g. "scientific research, statistical purposes, preservation of records for public interest, etc.," and for more information, see "Checklist ⑦."

Related provisions

Articles 15, 28-2 and 29-3 of the Act

Cf.

■ **For more information, see the guidebook, the 「Guideline on minimization of personal information collection (December 2020)」, the 「Guideline on pseudonymized information processing (September 2020)」, etc.**

5 When collecting personal information from sources other than data subjects for use in AI development, do you notify the source and purpose of processing at the request of data subjects? Legitimacy Participation

[YES / NO / N/A] ☐☐☐

Mandatory

➡ **When receiving personal information from a third party or collecting disclosed personal information, you must immediately inform data subjects that they have the right to demand the source, purpose of processing and suspension of processing at the request of data subjects.**

Check 1 **When collecting personal information from sources other than data subjects, did you check the source and purpose of processing?** (§ 20 of the Act) ☐☐☐

- When collecting personal information from a source other than data subjects, you are collecting it from an open source or a third party and processing it, and information you produced or generated on your own is excluded. (P. 135 of the handbook)

Check 2 **When you received personal information from a third party, did you check if the provider of the personal information collected and provided the personal information based on legitimate grounds?** (§ 3, § 17, § 71, etc. of the Act) ☐☐☐

- Personal information must be collected legitimately through the consent of data subjects, and used and provided within permitted purposes. In particular, receiving personal information for profit or illegal purposes while knowing it violates the law is prohibited.

Check 3 **When collecting disclosed personal information, did you check the purpose of disclosure, etc.?** (§ 3 of the Act, § 6③ and ④ of the standard guideline) ☐☐☐

- You can collect and use disclosed personal information within a reasonable scope when the data subject's consent is recognized according to the social norm in consideration of the intention and purpose of disclosure.

※ It is possible to check if it violates the law through comparison of the personal information controller's interests, data subjects' rights and public interests. (Cf.: [Supreme Court August 17, 2016, judgment, 2014-Da-235080, ruling])

Related provisions

Articles 3, 15, 17, 20 and 71 of the Act, Article 6 of the Standard Guideline, etc.

Cf.

■ **For more information, see the handbook (pp. 133~136), Supreme Court ruling (Supreme Court August 17, 2016, judgment, 2014-Da-235080), etc.**

3 Use and provision of personal information

6 **Did the use of personal information and provision of it to a third party meet the original purpose of collection throughout the AI development and operation process? If the personal information is used or provided beyond the original purposes, was there any other legitimate basis?**

Legitimacy

[YES / NO / N/A] ☐☐☐

Mandatory

➡ **In principle, personal information can be used and provided to a third party within the original purpose of collection. If personal information is processed for purposes other than the purpose of collection, there must be a separate basis.**

Within-Purpose Use and Provision of Personal Information

Check 1 **Does it fall under the original purpose* of collecting personal information?** (§ 15 and § 17 of the Act) ☐☐☐

* Personal information can be used and provided within the scope of the purposes of collection, e.g. the data subject's consent, conclusion and implementation of a contract.

Check 2 **Is it possible to use and provide personal information without additional consent reasonably in relation to the original purpose of collection?** (§ 15③ and § 17④ of the Act) ☐☐☐

- Matters pursuant to Article 14-2 of the Enforcement Decree, e.g. relevance to the original purpose of collection, predictability, data subjects' interests. infringement Y/N, securing safety, etc. , must be taken into consideration comprehensively.
- In this case, the personal information controller must disclose the judgment criteria for the considerations in the privacy policy in advance, and the privacy officer must check if the personal information is additionally used or provided according to the standards.

[**If used for development and enhancement of AI for the purpose of improving service**] As using the personal information, collected for the purpose of providing particular services, for the purpose of improving (enhancing, etc.) the services, has reasonable relevance to the original purpose of collection, and data subjects can predict it, and it is unlikely to wrongfully infringe on data subjects' interests, unless there are special circumstances, personal information can be used and provided without additional consent.

Out-of-Purpose Use and Provision of Personal Information

Check 3 **If using or providing personal information for purposes other than the original purpose of collection, did you receive separate consent from data subjects?** (§ 18② of the Act) ☐☐☐

- Even if consent to the collection and use of personal information was received, when personal information is used for purposes out of purpose, additional consent of data subjects is required.

Check 4 **Does it fall under an exceptional reason for out-of-purpose use and provision though it is difficult to receive consent?** (§ 18② of the Act) ☐☐☐

- If it is specially stipulated in the law / necessary for the protection of life, bodily or property interests

Check 5 **If personal information is pseudonymized as there is no basis for out-of-purpose use and provision, does it fall under the purposes permitted by law, e.g. scientific research?** (§ 28-2 of the Act) ☐☐☐

- Only for purposes, such as statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc., it is possible to process pseudonymized information without data subjects' consent. (For more information, see Checklist ⑦)

Related provisions

Articles 3, 15, 17, 18, 28-2 and 58-2 of the Act, Article 14-2 of the Enforcement Decree, etc.

Cf.

1. **For more information, see the handbook, the 「Guideline on online processing of personal information (December 2020)」, etc.**
2. **Reasonably considering time, cost and technology, even if other information is used, information that cannot identify particular individuals anymore (meaning anonymized information) will not be subject to laws. (§ 58-2 of the Act)**

7 If personal information is pseudonymized for AI development and operation without data subjects' consent, does it comply with the purposes and standards permitted by law? Legitimacy Safety

[YES / NO / N/A] ☐☐☐

Mandatory

➡ **The scope of using and providing pseudonymized information without data subjects' consent is limited for the purposes of statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc. Accordingly, you must check specific criteria, e.g. if you pseudonymize* personal information during AI development and operation as it is difficult to obtain consent to personal information processing is a purpose permitted by law, and comply with the obligation to prohibit re-identification.**

* "Pseudonymization" refers to making it impossible to identify particular individuals by deleting part of personal information or replacing all or part of it.

Check 1 **When pseudonymized information is processed without data subjects' consent, does the purpose fall under "statistical purposes, scientific research purposes, and archiving purposes in the public interest, etc."?** (§ 28-2① of the Act) ☐☐☐

- As it applies commonly to the pseudonymized information in "check items 2~8," it is necessary to clearly check it in advance.
- Scientific research: It refers to a study that applies scientific methods, e.g. development and demonstration of technology, basic researches, applied researches and private investment researches. (§ 2·8 of the Act)

[Scope of scientific research in relation to AI development and operation] In general, as scientific methods are applied to development of AI technology (modeling, learning, testing, etc.), it may be a scientific research, but it is difficult to deem AI-related service operation itself as a scientific research.

- If scientific methods, technology development and demonstration, are applied for the purpose of improving functions and enhancing algorithms during service operation, however, it may be a scientific research.
- Considering these points, as directly using others' pseudonymized information for service operation (disclosure, provision, etc.) is limited, to this end, the fact will be clearly notified to data subjects, and additional consent will be obtained, or the personal information will be pseudonymized.

Check 2 **Doesn't it include the personal information for which data subjects requested pseudonymization be suspended?** (§ 37 of the Act) ☐☐☐

- Data subjects may not exercise the right to demand suspension of pseudonymized information processing pursuant to Article 37 of the Act (§ 28-7 of the Act), but data subjects may demand suspension of pseudonymization before their information is pseudonymized. (p. 383 of the Handbook)

Check 3 **Do you check if the pseudonymized information you want to use is safely pseudonymized, and there is no risk of re-identification?** (§ 2·1·C and § 2·1-2 of the Act)

- Allowing pseudonymized information to be processed without assumes that personal information will be safely pseudonymized and there is no risk of re-identification without additional information.

[Precautions when AI learning data is pseudonymized] In general, as AI learning requires massive data processing, not only personal identification and attribute information, but also privacy data about particular individuals may be included.

- When personal information is pseudonymized for development of AI technology (learning, etc.) for the purpose of scientific researches, etc. without data subjects' consent, it is necessary to review the adequacy of pseudonymization and the possibility of privacy infringement
- To this end, it is necessary to apply a pseudonymization method, available at the current level of technology, depending on data type, safely pseudonymize learning data, and if any problem is found after adequacy review, and additionally pseudonymize personal information to ensure that data subjects' rights are not infringed

⇒ (Example) In case of SNS dialog data, it is necessary to pseudonymize not only the identification information* of the speaker, but also the identification information* of particular individuals included in the dialog or information on the concern about privacy infringement.

* For more information on examples of identification information and identifiable information, see the「Guideline on pseudonymization」(p. 17).

Check 4 **When providing pseudonymized information to a third party, do you exclude the information that can be used to identify particular individuals?** (§ 28-2② of the Act)

- In this case, information that can be used to identify particular individuals as well as additional information that can restore pseudonymized information to the original state should not be provided to a third party regardless of name, type or shape. (p. 222 of the Handbook)

[Limiting the disclosure of pseudonymized information related to AI development] If pseudonymized information is disclosed to unspecified individuals, whether the purpose of disclosure falls under statistical purposes, scientific research, preservation of records for public interest, etc. is unclear, and some of the unspecified individuals may have information that can identify particular individuals in combination with the disclosed information. So disclosure of pseudonymized information is virtually limited. (p. 224 of the Handbook)

⇒ If it is provided to an unspecified third party (disclosure, etc.), in principle, it must be pseudonymized. (p. 14 of the Guideline on processing of pseudonymized information)

⇒ If pseudonymized information is provided to a particular third party, the third party is responsible for the legitimacy of the purpose of processing pseudonymized information, prohibition of re-identification, and a separate contract regarding this may be concluded. (p. 223 of the Handbook)

Check 5 **Is combination of pseudonymized information performed through a specialized institution between different personal information controllers?** (§ 28-3 of the Act)

- Pseudonymized information, held by different personal information controller, must be combined through a combination specialist designated by the Personal Information Protection Commission or a related central administrative agency.

Check 6 **Do you take the technical, administrative and physical measures necessary for securing the safety of pseudonymized information?** (§ 28-4 of the Act)

- When pseudonymized information is processed, measures to secure the safety of personal information (§ 29 of the Act, and § 30 and § 48-2 of the Enforcement Decree) must be taken, and additional information for restoration to the original state must be separately stored and managed, and safety measures for pseudonymized information, e.g. separation of access rights to pseudonymized information and additional information, preparation and storage of related records (the purpose of processing pseudonymized information, pseudonymization items, details of pseudonymized information use, the recipient of personal information when it is provided to a third party, etc.), must be taken. (See § 29-5 of the Enforcement Decree (Measures to secure the safety of pseudonymized information))

Check 7 **Do you process pseudonymized information for the purpose of identifying particular individuals?** (§ 28-5 of the Act)

- Processing pseudonymized information for the purpose of identifying particular individuals is prohibited. A fine may be imposed on violators (less than three-hundredths of total sales), violators may be criminally punished (imprisonment with labor for not more than 5 years, or by a fine not exceeding KRW50 million). (§ 28-5①, § 28-6 and § 71 of the Act)

Check 8 When generating information that can identify particular individuals in the process of processing pseudonymized information, do you immediately stop processing, withdraw and destroy it?(§ 28-5② of the Act)

- If you do not stop using the information that can identify particular individuals, or do not withdraw or destroy it, you may be subject to an administrative fine not exceeding KRW30 million. (§ 75 of the Act)

Related provisions

Subparagraphs 1 and 1-2 of Article 2, Articles 28-2 ~ 28-7, 29, 71 and 75 of the Act, Articles 29, 29-2 ~ 29-6, 48-2 of the Enforcement Decree, etc.

Cf.

1. **As pseudonymized information is personal information, statutory obligations (safety measures, limiting out-of-purpose use and provision, etc.) will be applied equally.**
   - According to Article 28-7 of the Act, however, Articles 20, 21 and 27, Paragraph 1 of Article 34, Articles 35 through 37, 39-3, 39-4, 39-6 through 39-8 of the Act were not applied to pseudonymized information processed for the purpose of scientific research, etc..
2. **For more information, see the 「Guideline on processing of pseudonymized information (September 2020)」, etc.**

4 Storage and destruction of personal information

8 **Do you safely store and manage the personal information, used for AI development and operation through such measures as encryption and access control?** Safety

[YES / NO / N/A] ☐☐☐

Mandatory

➡ **Take the technical, administrative and physical measures*necessary for securing the safety of personal information in the AI development and operation process to prevent the unintended leakage misuse and abuse of personal information.**

* Safety measures, prescribed by law, e.g. establishment of internal control plans to prevent the loss, theft, leakage, forgery, alteration or damage of personal information, encryption, access control and management of access records

Check 1 **Do you establish and carry out internal control plans for safely processing personal information?** (§ 29 of the Act) ☐☐☐

- The internal control plan must include matters concerning the formation and operation of personal information protection organizations, e.g. designation of privacy officers, access control, encryption, security program installation and preparation of physical security devices.

Check 2 **Do you take measures, such as access control for personal information, limiting access rights and access record management?** (§ 29 of the Act, and § 30 of the Enforcement Decree) ☐☐☐

- See § 5, § 6 and § 8 of the 「Standards for measures to secure the safety of personal information」, and § 4 and § 5 of the 「Standards on the technical and administrative measures to protect personal information」.

Check 3 **Do you take measures, such as encryption of personal information, installation of security programs, and preparation of physical security devices for storage facilities?** (§29 of the Act, §30 and §48-2 of the Enforcement Decree)

- See §7 of the「Criteria for measures to secure the safety of personal information」, and §6 of the「Criteria for technical and administrative measures to protect personal information」.

Related provisions

Article 29 of the Act, Article 30 of the Enforcement,
Articles 4 through 12 of the「Criteria for measures to secure the safety of personal information (notification)」,
Articles 3 through 8 of the「Criteria for technical and administrative measures to protect personal information (notification)」, etc.

Cf.

1. **As the notifications related to safety measures stipulate the minimum standards necessary for securing safety, efforts to take additional measures need to be made in consideration of infringement risks due to personal information types, processing methods and characteristics of AI technology and service.**
2. **The standards for safety measures are differently stipulated depending on personal information controller types and amount of personal information (See the attached table of the「Standards for measures to secure the safety of personal information (notifications)」)**
3. **For more information, see the「Handbook on the standards for measures to secure the safety of personal information (December 2020)」, the「Handbook on the standards for the technical and administrative protection measures for personal information (December 2020)」, the「Guide to personal information encryption measures (December 2020)」, the「Guide to personal information protection measures (December 2020)」, etc.**

9 When personal information becomes unnecessary as AI development and operation ends, do you immediately destroy it? Safety

[YES / NO / N/A]

☐☐☐

Mandatory

➡ **Personal information, which becomes unnecessary as the retention period expires, the purpose of processing is accomplished, and people withdrew from membership, must be safely destroyed immediately beyond restoration, and if it must be preserved according to other laws, it must be stored and managed separately from other personal information.**

Check 1 **Do you safely destroy the unnecessary personal information beyond restoration?** (§ 21 of the Act and § 16 of the Enforcement Decree) ☐☐☐

- You must delete electronic files deleted permanently in a way that makes restoration impossible, and destroy printed matters by shredding or incinerating them so that it is impossible to restore or reproduce them.
- If personal information is pseudonymized, however, it can be used for such purposes as scientific researches for the minimum necessary period. (§ 28-7 of the Act)

Check 2 **If other laws require mandatory retention for a certain period of time, do you store it from other personal information?** (§ 21 of the Act) ☐☐☐

- If personal information is not destroyed and needs to be preserved according to other laws, the personal information or personal information files must be stored and managed separately from other personal information.

Check 3 **Do information and communications service providers, etc. destroy or separately store the personal information of users who have not used the online AI service for more than a year?** (§ 39-6 of the Act and § 48-5 of the Enforcement Decree) ☐☐☐

- If personal information is not destroyed or separately stored and managed without destruction, unless specially stipulated in the Act or other laws, they should not use or provide the personal information.

Related provisions

Articles 21, 28-7, 29, 37 and 39-6 of the Act, Articles 16 and 48-5 of the Enforcement Decree, etc.

Cf.

■ **For more information, see the handbook, the 「Guideline on online processing of personal information (December 2020)」, the 「Guideline on minimizing personal information collection (December 2020)」, etc.**

5 AI service management and supervision(regular)

10 **Do you manage, supervise and provide regular education for personal information handlers participating in AI development and operation?**

Responsibility

[YES / NO / N/A] ☐☐☐

Mandatory

➡ **Personal information controllers must safely process personal information within the scope of the authority granted to the persons in charge, e.g. developers, and manage, supervise and provide regular education for personal information handlers so that personal information is not misused or abused in the course of business.**

Check 1 **Do you designate privacy officer, and have and implement the personal information handler management and supervision system?** (§ 28 and § 31 of the Act) ☐☐☐

- Personal information controllers must designate privacy officers who will take responsibility for personal information processing, and appropriately manage and supervise personal information handlers, e.g. employees, temporary agency workers and part-time workers so that they can safely manage personal information when they handle it.

Check 2 **Do you provide regular personal information protection education for personal information handlers?** (§ 28 of the Act) ☐☐☐

- Personal information controllers must provide necessary regular education for personal information handlers to guarantee that personal information is handled appropriately.
- In particular, it is recommended to include the possibility of privacy infringement likely to occur due to personal information processing and countermeasures in the contents of the education.

Related provisions

Articles 28 and 31of the Act, Article 15 of the Standard Guideline, etc.

Cf.

1. **This self-checklist may be used as educational materials.**
2. **It is recommended that you should refer to the 「Guide to preventing exposure of personal information on homepages (November 2020)」, and internally share cases of leakage, exposure, misuse and abuse of personal information caused by employees intentionally or by mistake.**

11 When you outsource personal information process related to AI development and operation AI, do you do so in writing, and provide education for the outsourcees, and manage and supervise them?

[YES / NO / N/A] ☐☐☐

Mandatory

Responsibility Safety

➡ **When personal information processing is outsourced to a third party, you must document the purpose and scope of the outsourced work, safety measures and matters concerning liability for damages of the breach of fiduciary duty, and educate and supervise the outsourcee. In addition, you must include the details of the outsourced work and the outsourcee in the privacy policy and disclose them so that data subject can easily understand them.**

Check 1 **Did you include the scope of the outsourced work, safety measures and scope of responsibility in documents, such as the outsourcing agreement?** (§ 26 of the Act and § 28 of the Enforcement Decree) ☐☐☐

- When personal information processing is outsourced, you must include matters concerning "information on prohibition of processing personal information for purposes other than performance of the outsourced work, technical and administrative protection measures for personal information, etc." in the documents (the contract, etc.)

Check 2 **When outsourcing personal information processing, do you disclose the details of the outsourced work and the outsourcee?** (§ 26 of the Act and § 28 of the Enforcement Decree) ☐☐☐

- The personal information controller (outsourcer), who outsources personal information processing, must disclose the details of the outsourced work and the outsourcee in the privacy policy so that data subjects can easily check them anytime.

Check 3 **Do you manage and supervise the outsourcee's compliance with the law and education?** (§ 26 of the Act and § 28 of the Enforcement Decree) ☐☐☐

- The outsourcer must educate the outsourcee to prevent the loss, theft, leakage, forgery, alteration or damage of personal information due to the outsourcing, and supervise whether personal information is safely processed.

Related provisions

Article 26 of the Act, Article 28 of the Enforcement Decree, Article 15 of the Standard Guideline, etc.

Cf.

1. **You can use this self-checklist when managing and supervising the outsourcee's compliance with the law.**
2. **For more information, see the 「Handbook on the outsourcing of personal information processing (December 2020)」, etc.**

6 AI service user protection and damage relief(regular)

12 **During AI development and operation, do you include and write the details of personal information processing in the privacy policy, and disclose them in the homepage, etc.?** Transparency

[YES / NO / N/A] ☐☐☐

Mandatory

➡ **As data subjects may have difficulty understanding how their personal information is processed due to the opacity of AI service operation, the personal information controller must specifically include the information on personal information processing in the privacy policy, and disclose it in the homepage, etc. so that data subjects can easily understand it.**

Check 1 **Did you include the mandatory information* in the privacy policy?** (§ 30 of the Act and § 31 of the Enforcement Decree) ☐☐☐

* Personal information processing items, the purpose of processing, retention period, provision of personal information to a third party, outsourced items, information on measures to secure safety, privacy officers, grievance department, information on data subjects' exercise of rights, information on installation and operation of the automatic personal information collection system (Internet access information file, etc.) and the denial thereof, etc.

Check 2 **Do you continuously disclose new and revised privacy policies on the Internet homepage, etc.?** (§ 30 of the Act and § 31 of the Enforcement Decree) ☐☐☐

- The name will be the 'privacy policy' but you must use font size and color to differentiate it from other notifications (terms and conditions, information on copyright, etc.) so that data subjects can easily check it.

Related provisions

Article 30 of the Act, Article 31, of the Enforcement Decrees, Articles 18 through 21 of the Standard Guidelines, etc.

Cf.

1. **As the preparation and disclosure of the privacy policy and data subjects' consent are two different matters, you must be sure not to include the consent to collection and use of personal information in the privacy policy and provide only the link, and substitute it for consent.**
2. **For more information, see the Handbook, the 「Guideline on establishing the personal information processing policy (December 2020)」, etc.**
3. **Refer to the specific and easy-to-understand privacy policies of similar industries**

13 Do you have and carry out the procedure for processing data subjects' request to exercise their rights, e.g. access to, correction, deletion and suspension of processing of the personal information processed in AI service? Participation

[YES / NO / N/A] ☐☐☐

Mandatory

➡ **As it is difficult to know how personal information is processed or predict results oftentimes due to the characteristics of AI technology, the personal information controller will review the possibility of meeting data subjects' request to exercise their rights (access, connect, delete, suspend processing, etc.) and countermeasures in advance.**

- As data subjects' rights, stipulated by the law, falls under data subjects' 'right to informational self-determination,'[4] which is guaranteed by the Constitution, you must make sure that they are not infringed.

Check 1 **Do you have and implement the specific methods and procedures for accessing, correcting, deleting and suspend the processing of personal information?** (§3, §4 and §35~38 of the Act and §41of the Enforcement Decree) ☐☐☐

- The personal information controller must prepare the method and procedure for data subjects' exercise of the rights, e.g. request access to personal information, and in this case, the personal information controller must provide easy-to-use methods, e.g. in writing and by phone and e-mail.
- If it is difficult to meet the needs of data subjects as it is difficult to separately identify and extract particular personal information due to the characteristics of AI technology and data, you must provide sufficient information, e.g. the reason and alternatives.

4 **right to informational self-determination**: Data subjects' right to determine when their personal information will be known to whom and used to what extent for themselves, that is, data subjects' right to control and determine the disclosure and use of personal information on their own

• Foreign countries are reinforcing guarantee of AI-related rights of data subjects besides access, correction, deletion and suspension of processing.

[An example of automated AI-related decision-making] In case of AI service, as it is difficult to predict AI's internal personal information processing due to automation of data processing, complexity, opacity, etc., you need to make efforts to guarantee data subjects' rights according to the principles of personal information protection. In relation to this, EU GDPR[5] notifies the presence of automated decision-making to data subjects to protect data subjects' rights, and stipulates the right to demand explanation about the decision and object to it.

Check 2 **Do you disclose how data subjects can exercise their rights in the privacy policy?** (§ 30 of the Act) ☐☐☐

• Information on data subjects' rights and obligations, and how to exercise them must be included in the privacy

Related provisions

Articles 1, 3, 4, 30, 35, 36, 37 and 38 of the Act, Articles 41 through 44 of the Enforcement Decree, Articles 31, 34 and 44 of the Standard Guideline, policy.

Cf.

1. **See the provisions that stipulate the requirements for limiting data subjects' exercise of rights (§ 35~37 of the Act).**
2. **For more information, see the Handbook, etc.**

5 **EU GDPR (General Data Protection Regulation)**: EU (European Union)'s Personal Information Protection Act

14 When personal information is leaked during AI service operation, do you have and carry out the procedure for notification to data subjects, reporting leakage and support for damage relief? Responsibility Safety

[YES / NO / N/A] ☐☐☐

Mandatory

➡ **In consideration of the characteristics of AI technology and service, you must review the impact of personal information leakage on users and countermeasures in advance, and prepare a manual, and quickly respond to leakage.**

Check 1 **In consideration of the characteristics of AI technology and service, did you figure out the impact of personal information leakage on data subjects?** (§ 34 and § 39-4 of the Act) ☐☐☐

- You must figure out the possibility of personal information leakage and the impact of personal information leakage on data subjects in advance for each stage of AI service, and establish ways to minimize the impact on data subject.

Check 2 **Do you have and practice the personal information leakage response manual?** (§ 34 and § 39-4 of the Act and § 39 and § 48-4 of the Enforcement Decree) ☐☐☐

- Depending on your status e.g. personal information controller or information and communications service provider, you consider that different provisions are applied report targets (number of leaks), and when to notify data subjects, and reflect them in the manual.

Classification	Report targets (number of leakage), when to report, etc.
Personal information controller	• If the personal information of more than 1,000 persons, you must immediately (within 5 days) notify data subjects, and report the results of measures taken to the Personal Information Protection Commission and KISA. • Related provisions: § 34 of the Act, § 39 and § 40 of the Enforcement Decree, § 26 of the Standard Guideline, etc.
Information and communications service provider, etc.	• If personal information is leaked, regardless of the size of the leakage, you must notify it to users within 24hours, and report it to the Personal Information Protection Commission and KISA. • Related provisions: § 39-4 of the Act, § 48-4 of the Enforcement Decree, etc.

Check 3 **If you become aware of personal information leakage, do you immediately notify it to data subjects, and are you ready to take necessary measures?** (§ 34 and § 39-4 of the Law, and § 40 of the Enforcement Decree)

- In case of information leakage, you must notify leaked items, when and how they were leaked, how to minimize damage, how to report damage, and the damage relief procedure to data subjects, and take necessary measures.

Related provisions

Measures in Articles 34 and 39-4 of the Act, Articles 39, 40 and 48-4 of the Enforcement Decree, Articles 25 through 29 of the Standard Guideline, etc. must be taken.

Cf.

1. **For more information, see the 「Manual for responding to personal information leaks (December 2020)」, etc.**
2. **Personal information protection portal (www.privacy.go.kr): See "Minwon Madang, Reporting personal information leakage and infringement."**

7 Autonomous personal information protection activities (regular)

15 **Do you actively carry out autonomous personal information protection activities during AI development and operation?** Responsibility Fairness Transparency Safety

[YES / NO / N/A] ☐☐☐

Recommended

➡ **As AI technology continues to advance, a lot of personal information is collected and use for various services using this technology. Given this background, the personal information controller and the personal information handler must be aware of the importance of personal information protection, and proactively carry out autonomous protection activities to prevent privacy infringement, e.g. unexpected personal information leakage.**

Check 1 **Do you consider personal information protection during I technology development and service?** (§ 3 of the Act) ☐☐☐

- For reliable AI development and operation, personal information protection is essential.

Check 2 **Do you explain and disclose how AI service works, and how personal information is utilized in an easy-to-understand way?** (§ 3 of the Act) ☐☐☐

- You can disclose how AI service works to users in an easy-to-understand way and secure reliability.

Check 3 **Are you making efforts to minimize personal information infringement through anonymization and pseudonymization?** (§ 3⑦ of the Act) ☐☐☐

- When it is possible to achieve the purpose of collecting personal information by anonymizing or pseudonymizing personal information, the personal information controller must make efforts to minimize personal information infringement and enhance safety, i.e. anonymizing personal information, if anonymization is possible, and pseudonymizing personal information if it is impossible to achieve the purpose through anonymization

Check 4 **Do you constantly monitor and improve the possibility of privacy infringement, unintended personal information leakage, etc. during AI development and operation?** (§ 3⑥ of the Act) ☐☐☐

- In consideration of the characteristics of AI technology and service, the personal information controller must minimize privacy infringement due to personal information processing, and constantly monitor whether there is any risk of personal information leakage, and carry out improvement activities if there are problems

Check 5 **Do you have the work and organizational system for receiving, reviewing and responding to users' suggestions (opinions), inquiries and objections in regard to the personal information processing during AI technology and service operation?** (§3⑥ and §3⑧ of the Act)

- It is possible to secure the reliability of service by reflecting users' opinions with a communication system related to the personal information processing of AI services and products

Related provisions

Paragraphs 6 through 8 of Article 3 of the Act, Article 4 of the Standard Guidelines, etc.

Cf.

1. **It is recommended to develop and apply the "technology for reinforcing personal information protection"* fit for the AI development and operating environment.**
   * As the PET (Privacy-Enhancing Technologies) technology for reinforcing privacy protection is continuously researched and developed at home and abroad, it is possible to refer to various cases.
2. **See key issues, including cases of personal information infringement related to domestic and overseas AI technology and service.**
3. **Sharing key issues and response plans through organizations in related areas, including self-regulatory organizations**

8 AI ethics inspection (regular)

16 **Do you constantly monitor and improve ethical issues related to personal information processing during AI development and operation?** Fairness

[YES / NO / N/A]

Recommended

➡ **You must constantly monitor so that there are not ethical issues, e.g. social discrimination and bias due to personal information processing during AI development and operation, and quickly respond to problems.**

Check 1 **[Planning and design stage] Do you check the ethical issues likely to occur during AI development and operation, and reflect the response plans in the design?**

- You must review the various issues likely to occur when processing data including personal information in the AI technology development and service planning and design process, and come up with a response plan.

Check 2 **[Test stage] Do you check if the Ai model has any issues, e.g. social bias and discrimination, and make improvements?**

- If AI model development is completed, you must review the possibility of issues, such as social discrimination and bias, through repeated tests, and improve the issues you found before the service is launched.

Check 3 **[Service operation stage] Do you continuously monitor where there are any issues, e.g. privacy infringement and discrimination, during AI service operation, and quickly respond to problems?**

- You must constantly monitor to make sure there are no problems, such as privacy infringement and discrimination, due to the processing of sensitive information during AI service operation, and quickly respond to problems.

Check 4 **[Data management] Do you manage the quality of learning data and risks to minimize social discrimination during personal information processing?**

- As bias of the AI learning data affects service operation as well, you must minimize the occurrence of ethical issues related to data by managing the quality of data and risks from the development stage.

Cf.

1. **For more information, see the "People-centric 「AI Ethical Standards」."**
2. **Detailed judgment criteria for ethical issues, e.g. social discrimination, will be published later in the form of a checklist. (Ministry of Science and ICT)**

Information on utilization

1. AI developers and operators can use the self-checklist as a guideline for pre-inspection you must know for personal information protection, and as an educational material for chief privacy officers (CPO) or field workers in AI –related industrial sites.

   ※ As it contains the major guidelines pursuant to the 「Personal Information Protection Act」, personal information controllers in areas other than AI service can use this checklist autonomously.

2. As the specific methods of implementing the mandatory and recommended items included in the self-checklist may vary depending on personal information processing types and methods, you can use it with reference to the provisions in related laws and notifications*, “the handbook on personal information protection laws, guidelines and notifications (December 2020)”, and related materials**, e.g. guidelines.

   * Laws, enforcement decrees, notifications, etc. related to personal information protection: See Korean Law Information Center (law.go.kr).

   ** See the following website.

3. For information on counseling related to self-checklist and inquiries about personal information protection laws, contact the ‘Personal Information Infringement Report Center’(privacy.kisa.or.kr or call 118).

4. The checklist will be continuously supplemented by reflecting the revisions in laws related to personal information protection and changes in the AI technology and environment, and the latest information on the personal information protection handbook, guides and guidelines is posted on the following website*.

   * “Personal Information Protection Commission website (www.pipc.go.kr)” (policies, laws /legal information/guides and guideline) “personal information protection portal (www.privacy.go.kr)” (archive/instructional materials)

5. As ethical issues, e.g. AI-related privacy infringement, social discrimination and bias, are actively discussed at home and abroad, the Personal Information Protection Commission is planning to cooperate with related agencies to respond to this

Appendix

Glossary

- **Artificial intelligence (AI)** It is science and technology for implementing human intelligence with computers. It includes the ability to ① recognize the situation, ② judge and act rationally and logically, and ③ perform emotional and creative functions. (Related ministries, national artificial intelligence strategy (December 2019))
- **Artificial intelligence (AI) service** All services providing various functions based on the AI technology to achieve a specific purpose
- **Personal information** Information relating a living individual. Information that identifies a particular individual by his or her full name, resident registration number, image, etc., or 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 (Subparagraph 1 of Article 2 of the 「Personal Information Protection Act」 (hereinafter referred to as the 'Protection Act')

  ※ In this case, to check whether the information can be easily combined, the time it takes to identify an individual, the cost and technology, e.g. the possibility of acquiring other information, must be considered reasonably.
- **Privacy by design (PbD) principle** It means application of the technology and policy for protecting privacy and personal information throughout the life cycle from the planning stage to the destruction stage. It consist of 7 principles: ① prevention, not follow-up measures, ② taking measures to protect privacy from the initial settings, ③ design including privacy protection, ④ balance between privacy protection and business function, ⑤ protection of personal information throughout its life cycle, ⑥ maintaining the visibility and transparency of personal information processing, and ⑦ respect for user privacy.
- **Sensitive information** Information on ideology, creed, joining and withdrawal from labor unions and political parties, political views, health, sex life, and personal information highly likely to infringe the privacy of data subjects as stipulated by the 「Personal Information Protection Act enforcement decrees」(hereinafter referred to as the 'Enforcement Decree') (Article 18 of the Enforcement Decree)
- **Personally identifiable information** Identification information assigned to uniquely distinguish individuals according to laws as stipulated by the Enforcement Decree of the Personal Information Protection Act (Article 19 of the Enforcement Decree)
- **Data subject** An individual who is identifiable through the information processed and is the subject of that information (Subparagraph 3 of Article 2 of the Protection Act)
- **Personal information controller** A public institution, legal person, organization and individual that processes personal information directly or indirectly to operate the personal information files as part of its activities (Subparagraph 5 of Article 2 of the Protection Act)

- **Personal information handler** A person who processes personal information under the command and supervision of the personal information controller, e.g. an employee, temporary agency worker and part-time worker, so that personal information can be safely managed in processing personal information (Paragraph 1 of Article 28 of the Protection Act)
- **Information and communications service providers** A telecommunications business entity and any other person who provides information or intermediates to provide information commercially by utilizing services provided by a telecommunications business entity (Subparagraph 3 of Paragraph 1 of Article 2 of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.)
- **Pseudonymized information** Information that is incapable of identifying a particular individual without the use or combination of information for restoration to the original state (Item C of Subparagraph 1 of Article 2 of the Protection Act)
- **Pseudonymization** A procedure to process personal information so that the information cannot identify a particular individual without additional information, by deleting in part, or replacing in whole or in part, such information (Subparagraph 1-2 of Article 2 of the Protection Act)
- **Combination agency** A specialized institution designated by the head of the Personal Information Protection Commission or a related central administrative agency to combine pseudonymized information between different personal information controllers
- **Anonymized information** Information that no longer identifies a certain individual when combined with other information, reasonably considering time, cost, technology, etc. (Article 58-2 of the Protection Act)
- **Additional information** The means or method used to replace all or part of the personal information, and information that can restore deleted or replaced personal information through comparison with pseudonymized information
- **Re-identification** Identifying a particular individual from information that is pseudonymized to make him/her unidentifiable
- **Biometrics** Personal information resulting from specific technical processing of data relating to the physical, physiological or behavioral characteristics of an individual for the purpose of uniquely identifying that individual (Subparagraph 3 of Article 18 of the Enforcement Decree)
- **Outsourcing of personal information processing** It means that the personal information controller (outsourcer) outsources personal information processing, e.g. collection and use, to a third party (outsourcee), or the works accompanied by personal information processing, e.g. use and provision, to the outsourcee
- **Privacy policy** A document that includes the personal information controller's personal information processing standards and protection measures as well as the details in Article 30 of the Protection Act
- **PET** It is short for Privacy-Enhancing Technologies. A technology that empowers individuals and implements the personal information protection principles by minimizing utilization of personal information and emphasizing protection

Major domestic and overseas AI ethical principles

Trends in discussions of AI ethics at home and abroad

- The government agencies, international organizations and enterprises of major countries are announcing and actively discussing ethical recommendations concerning AI and personal information protection guidelines.

Major domestic and overseas AI ethical principles

Classification		Publisher	Title (year published)
Overseas	International organizations	OECD, G20	Artificial intelligence principles (2019)
	Singapore	Personal Information Protection Commission	Artificial intelligence governance framework model (2020)
		Personal Information Protection Commission	A written opinion on artificial intelligence and personal information (2018)
	US	Federal Trade Commission	A guideline on artificial intelligence and algorithm (2020)
		National Institute of Standards and Technology	Four Principles of Explainable Artificial Intelligence (2020)
	EU	European Commission	A guideline on reliable artificial intelligence (2019)
			Artificial Intelligence Act (2021)
		EDPS, CNIL, Garante	Declaration on Ethics and Data Protection in Artificial Intelligence (2018)
	Canada	Office of the Privacy Commissioner of Canada	Guidelines on Automated Individual Decision-Making (2020)
			Proposals for ensuring appropriate regulation of artificial intelligence (2019)
	Germany	Data Protection Authority	7 principles of artificial intelligence (2019)
	France	Commission Nationale de l'Informatique et des Libertés	Chatbots: les conseils de la CNIL pour respecter les droits des personnes (2021)
		Commission Nationale de l'Informatique et des Libertés	Recommendations on ethical issues of algorithm and artificial intelligence (2018)
	UK	Information Commissioner's Office	Guidance on AI and Data protection (2020)
		Alan Turing Institute	A Guideline on Understanding Artificial Intelligence Ethics and Safety (2019)
	Australia	Commonwealth Scientific and Industrial Research Organisation	8 principles on artificial intelligence (2019)
	China	China Information Security Standardization Technical Committee	A cyber security action guide to prevention of artificial intelligence ethical security risks (2021)
		Special Committee on Next-generation Artificial Intelligence Management	Principles for management of next-generation artificial intelligence (2019)
	Japan	Cabinet Secretariat	Principles for realizing a human-centered artificial intelligence society (2019)
	Hong Kong	Privacy. Commissioner for Personal Data	Ethical Accountability Framework for Hong Kong, China (2018)
Domestic	Korea	Ministry of Science and ICT	Human-centric AI ethical standard (2020)
		Korea Communications Commission	Principles for user-centric intelligent information society (2019)
		Naver	Naver AI Code of Ethics (2021)
		Kakao	Algorithm Ethics Charter (established in 2018, revised in 2019 and 2020)

※ See the information of https://repository.sapi.co.kr <Seoul National University artificial intelligence policy initiative AI ethical principles index>, https://kaiea.org/research < Korea Artificial Intelligence Ethics Association Research Archive>, etc.

※ European Commission proposed the 'provision for establishing harmonious AI rules' (AI Act) (April 2021). Major countries are discussing and researching enactment of AI-Related provisions.

People-centric 「Artificial intelligence (AI) ethical standard」
(December 2020, Ministry of Science and ICT)

Artificial intelligence ethical standards: 3 basic principles and 10 key requirements

1) 3 basic principles – Principles to be considered in the process of developing and utilizing artificial intelligence

⬡ 3 basic principles as standards that must be considered in all processes ranging from AI development to utilization for the sake of 'AI for Humanity'

❶ The principle of human dignity

- A human being is a living organism that has a body and reason and cannot be replaced by mechanical products developed for humans including artificial intelligence.
- Artificial intelligence must be developed and utilized to the extent that it does not harm human life, nor mental and physical health.
- Development and utilization of artificial intelligence must be safe and robust enough not to harm humans.

❷ The principle of the public good of society

- The society as a community pursues the value of the well-being and happiness of as many people as possible.
- Artificial intelligence must be developed and utilized to guarantee accessibility to the socially underprivileged and vulnerable who can be easily alienated in the intelligent information society.
- Development and utilization of artificial intelligence for promotion of public interests must be able to improve the universal welfare of mankind from the social, national and global perspective.

❸ The principle of the purposiveness of technology

- AI technology must be developed and utilized in line with the purpose and intention of being a tool necessary for human life, and the process must be ethical.
- Development and utilization of artificial intelligence for the life and prosperity of mankind must be encouraged and promoted.

2) 10 key requirements – detailed requirements for realizing the basic principles

10 key requirements, which must be met throughout the life cycle of artificial intelligence, are presented to practice and implement the 3 basic principles.

❶ Human Rights Guarantee

- Development and utilization of artificial intelligence must respect the rights granted equally to all humans, and guarantee the rights specified in various democratic values and international human rights law.
- Development and utilization of artificial intelligence should not infringe on the rights and freedom of humans.

❷ Privacy protection

- The privacy of individuals must be protected in all artificial intelligence development and utilization processes.
- Efforts must be made to minimize abuse of personal information throughout the life cycle of artificial intelligence.

❸ Respect for diversity

- The diversity and representative nature of users must be reflected in all artificial intelligence development and utilization processes, and bias and discrimination in terms of individual characteristics, e.g. gender, age, disability, region, race, religion, and state must be minimized, and commercialized artificial intelligence must be applied fairly to everyone.
- Accessibility to artificial intelligence technology and service must be guaranteed for the socially underprivileged and vulnerable, and efforts must be made to distribute the benefits of artificial intelligence to everyone, not a particular group.

❹ Prohibition of infringement

- Artificial intelligence should not be used for the purpose of directly harming humans.
- Efforts must be made to prepare countermeasures to the risks and negative results of artificial intelligence.

❺ Public interests

- Artificial intelligence must be used not only for pursuit of personal happiness, but also for promotion of social and public interests and for the common good of mankind.
- Artificial intelligence must be used in a way to lead to positive social changes.
- Education must be provided in various ways to maximize the positive functions of artificial intelligence and minimize its negative functions.

❻ Solidarity

- The relational solidarity among various groups must be maintained, and artificial intelligence must be used in full consideration of future generations.
- Fair opportunities for participation must be guaranteed for various groups throughout the life cycle of artificial intelligence.
- The international community must make efforts to cooperate in development and utilization of ethical artificial intelligence.

❼ Data management

- Data, including personal information, must be used in conformity with the purposes, and should not be used beyond such purposes.
- Data quality and risks must be managed so that data bias can be minimized in the data collection and utilization process.

❽ Responsibility

- Efforts must be made to minimize damage by establishing subjects of responsibility in the process of developing and utilizing artificial intelligence.
- Responsibilities of artificial intelligence designers and developers, service providers and users must be clearly defined.

❾ Safety

- Efforts must be made to prevent potential risks and guarantee safety in the process of developing and utilizing artificial intelligence.
- When there are obvious errors or infringement in the process of utilizing artificial intelligence, efforts must be made to enable users to control the function.

❿ Transparency

- To build social trust, in consideration of conflicts with other principles, efforts must be made to ensure a level of transparency appropriate for utilization of artificial intelligence and enhance explainability.
- When providing AI-based products or services, details of AI activities and risks likely to occur in the utilization process must be notified in advance.

Published on May 31, 2021

Publisher: Personal Information Protection Commission

Supporting organization: Korea Internet & Security Agency

- This self-checklist (version 1.0) was prepared on May 31, 2021.
- Privacy infringement prevention measures in AI service will be continuously updated in reflection of revisions of laws related to personal information protection and changes in technology and environment.
- You can check the latest data in “Personal Information Protection Commission website (www.pipc.go.kr)” and the “personal information protection portal (www.privacy.go.kr).”