SHIN&KIM
법무법인(유) 세종

# PIPC Issues Guidelines on the Processing of Personal Information for the Development and Use of Generative AI

2025.08.14

On August 6, 2025, the Personal Information Protection Commission (**PIPC**) issued the *Guidelines on the Processing of Personal Information for the Development and Use of Generative AI* (the **Guidelines**). The Guidelines are intended to provide authoritative clarification regarding the application of the *Personal Information Protection Act* (**PIPA**) to all stages of the generative AI lifecycle and to strengthen the capacity of private-sector entities and public institutions to ensure voluntary and proactive compliance with statutory requirements.

## 1. Overview

The Guidelines classify the generative AI lifecycle into four distinct phases: (i) objective setting, (ii) strategy formulation, (iii) AI training and development, and (iv) system deployment and management. For each phase, the Guidelines identify key issues pertaining to the processing of personal information, specify the relevant legal obligations under the PIPA, and set forth the requisite technical and organizational measures to be implemented. The Guidelines further underscore the necessity of establishing a comprehensive AI privacy governance framework to ensure uniform and systematic compliance throughout the entirety of the AI lifecycle.

## 2. Key Considerations at Each Stage of Generative AI Development and Use

### (1) Objective Setting

- The purpose of the generative AI system must be defined with specificity, taking into account the intended use

case, target user base, and inherent technical limitations. This includes: (i) clearly identifying the intended uses of the system, (ii) anticipating foreseeable misuse, and (iii) recognizing and documenting operational constraints in advance.

- Upon defining the purpose of processing, a valid legal basis under the PIPA must be established. Where publicly available personal information is processed for training generative AI, the legal basis of "legitimate interests" under Article 15(1)(vi) of the PIPA may be relied upon.For user personal information, if the processing remains within the scope of the purpose for which the personal information was originally collected (**original purpose**), the existing legal basis—such as the data subject's consent, contractual necessity, or legitimate interests—may be maintained.Otherwise, compliance requires either: (i) invoking the "additional use" provision under Article 15(3) with a demonstrable nexus to the original purpose; (ii) implementing de-identification measures under Articles 28-2 and 58-2; or (iii) establishing a separate legal basis for processing beyond the original purpose in accordance with Article 18(2).

## (2) Strategy Formulation

- Once the scope of processing and legal basis have been determined, the organization should establish: (i) the development and use methodology, (ii) whether further model training (e.g., fine-tuning) will be undertaken, (iii) data quality assurance mechanisms, and (iv) risk mitigation and governance measures.
- Large Language Model (**LLM**) development generally proceeds through one of three approaches: (i) use of commercial AI services, (ii) deployment of publicly available models, or (iii) proprietary in-house development. In all cases, the privacy-by-design (**PbD**) principle must be integrated from the outset.
- Where the processing involves large-scale or sensitive personal information, a Personal Information Impact Assessment (**PIIA**) is advisable. For generative AI-related PIIAs, existing frameworks should be tailored to address AI-specific risks, including:
- **1. Personal information flow analysis** – mapping the lifecycle of personal information from collection to training, inference, and output generation;
- **2. Risk factor assessment** – addressing conventional privacy risks alongside risks unique to generative AI (e.g., inference attacks, hallucinations, and data leakage); and
- **3. Mitigation planning** – identifying safeguards to reconcile AI innovation with effective protection of data subjects' rights.

## (3) AI Training and Development

- Generative AI systems may inadvertently reproduce original personal information or generate outputs that infer sensitive attributes, thereby creating risks to data subjects' rights and freedoms. Safeguards should be implemented at the following levels:

| Level | Key Considerations |
|---|---|
| Data level | • Mitigate risks of contamination, bias, and inaccuracy<br>• Exclude public content explicitly marked with "no scraping" directives<br>• Remove, pseudonymize, or anonymize sensitive data prior to training |
| Model level | • Apply fine-tuning and alignment techniques to improve safety<br>• Implement safeguards against adversarial or model inversion attacks |

| | |
|---|---|
| System level | • Enforce access controls, particularly for external API integrations<br>• Apply input/output filtering mechanisms<br>• Implement heightened safeguards when interfacing with external databases (e.g., Retrieval-Augmented Generation; **RAG**) |

### (4) System Deployment and Management

- Privacy compliance obligations under the PIPA extend beyond the development phase. Prior to deployment, systems must undergo operational testing to validate accuracy, robustness, and compliance, with any identified privacy risks remediated before release. An Acceptable Use Policy (**AUP**) should be adopted, publicly disclosed, and enforced to mitigate risks of misuse.
- Following deployment, organizations must:
- 1. Establish accessible channels for the reporting and remediation of inappropriate or harmful outputs;
- 2. Respond in a timely and compliant manner to data subjects' exercise of rights under the PIPA, including the right to object to automated decision-making and the rights to request an explanation or a review; and
- 3. Maintain transparency by disclosing personal information processing practices through Privacy Policies, FAQs, and other suitable public-facing materials.

## 3. AI Privacy Governance Framework

- Having regard to the increasing complexity and scale of personal information processing inherent in generative AI systems, organizations should establish and maintain a formal internal governance framework—under the leadership and accountability of the Chief Privacy Officer (**CPO**)—to ensure continuous compliance with applicable personal information protection laws and regulations.
- The governance framework should encompass, at a minimum, the following components:
- **1. CPO-led Oversight** – A governance structure that vests the CPO with clearly defined authority and responsibility to supervise, direct, and monitor personal information processing activities throughout all phases of the generative AI lifecycle, ensuring both legal compliance and information security.
- **2. Ongoing Risk Assessment** – Systematic and periodic evaluation of privacy risks associated with generative AI, employing tools and methodologies, such as PIIAs and adversarial testing (e.g., red teaming).
- **3. Cross-Functional Coordination** – Formalized collaboration between the CPO, the Chief Artificial Intelligence Officer (**CAIO**), the Chief Information Security Officer (**CISO**), and other relevant senior officers to ensure integrated and cohesive oversight of AI development, deployment, and operation.
- **4. Early-Stage Privacy-by-Design Implementation** – Integration of PbD principles from the earliest stages of system planning and development, embedding appropriate technical and organizational safeguards into AI systems and services by default.

## 4. Key Takeaways

The Guidelines supplement the statutory obligations set forth under the PIPA by prescribing additional technical, organizational, and procedural measures designed to proactively safeguard personal information across all stages of the generative AI lifecycle. They serve as an authoritative reference for the establishment of a robust and comprehensive privacy management framework.

The stage-specific considerations articulated in the Guidelines are inherently interrelated and must be operationalized within a unified and integrated governance structure. This, in turn, requires the establishment of a formal AI privacy governance framework and, where appropriate, the re-definition and enhancement of the authority, duties, and accountability of the CPO. Depending on the organization's operational and governance context, this may involve the creation of a dedicated AI governance body or the comprehensive review and strengthening of existing governance mechanisms.

The imperative for such governance is further highlighted by the forthcoming *Act on the Development of Artificial Intelligence and Establishment of Trust* (**AI Basic Act**), which will impose mandatory requirements for the implementation of management systems designed to ensure the reliability and safety of AI systems.

Given the rapid pace of technological advancement in AI and the corresponding escalation of privacy, security, and operational risks, organizations engaged in the development or deployment of generative AI should maintain ongoing monitoring of the Guidelines and remain abreast of applicable laws, regulatory guidance, and policy developments, ensuring timely adaptation of their compliance and governance measures.

[Korean version] 개인정보보호위원회, '생성형 인공지능(AI) 개발활용을 위한 개인정보 처리 안내서' 배포

## Key Contacts


### Sinook Kang
Senior Partner

+82-2-316-4059
sokang@shinkim.com

### Jeong Ho Ahn
Partner

+82-2-316-2891
jhahn@shinkim.com

### Joe Juneyoung Jang
Partner

+82-2-316-4985
jyojang@shinkim.com

### Ho Sang Yoon
Partner

+82-2-316-2584
hsyoon@shinkim.com

**Keunho Kim**
Associate

+82-2-316-1926
kehkim@shinkim.com

**Soonyoung Heo**
Foreign Attorney

+82-2-316-1837
syheo@shinkim.com