SHIN&KIM
법무법인(유) 세종

개인정보보호위원회, '생성형 인공지능(AI) 개발활용을 위한 개인정보 처리 안내서' 배포

2025.08.14

개인정보보호위원회는 2025년 8월 6일 '생성형 인공지능(AI) 개발활용을 위한 개인정보 처리 안내서'를 배포하였습니다. 본 안내서는 생성형 인공지능 개발과 활용의 전 과정에서 개인정보보호법 적용의 불확실성을 해소하고, 기업기관의 자율적 법준수 역량을 높이고자 하는 취지에서 마련되었습니다. 이하에서는 본 안내서의 주요 내용을 자세히 살펴보도록 하겠습니다.

1. 개요

본 안내서는 생성형 AI 수명주기를 ① 목적 설정, ② 전략 수립, ③ AI 학습 및 개발, ④ 시스템 적용 및 관리 단계로 구분하며, 각 단계별로 고려해야 할 개인정보 이슈 및 이에 따른 법적 기준, 안전조치 등을 제시하고 있습니다. 이와 함께 모든 단계에 걸쳐 개인정보 관련 법규 준수를 위해 필요한 AI 프라이버시 거버넌스 체계에 대해서도 함께 안내하고 있습니다.

2. 생성형 AI 개발활용 단계별 주요 내용

(1) 목적 설정

- 개인정보의 처리 목적 획정 및 리스크 관리를 위해서 생성형 AI의 사용 맥락, 대상, 기술적 한계 등을 고려해 **생성형 AI의 목적을 구체화해야 합니다**. 이를 위해서는 AI의 의도된 용례(intended use)를 명확히 정의하고, 예견 가능한 오용(foreseeable misuse) 등 한계점을 사전에 파악해야 합니다.
- **개인정보 처리 목적을 구체화하였다면 적합한 적법근거를 마련해야 합니다**. 생성형 AI 학습에 공개된 개인정보를 활용하는 경우에는 정당한 이익(법 제15조 제1항 제6호)을 적법 근거로 활용할 수 있으며 이용자 개인정보를 활용하는 경우에는 기존 수집목적 범위 내에 있다면 기존의 동의, 계약, 정당한 이익 등을 적법 근거로 할 수 있고, 그 외에는 수집목적과의 합리적 관련성 등을 고려하여 추가적 이용 조항(법 제15조 제3항)을 근거로 하거나 비식별화 조치(법 제28조의2 및 제58조의2) 또는 목적 외 이용을 위한 적법 근거를 마련해야 합니다(개인정보 보호법 제18조 제2항).

(2) 전략 수립

- 개인정보 처리의 범위와 적법 근거를 구체화하였다면, **▲ 생성형 AI의 개발활용 방식, ▲ 미세조정 등 추가학습 여부, ▲ 데이터 품질 확보, ▲ 리스크 관리 방안 등 후속 의사결정의 방향을 구체화해야 합니다**.
- LLM 기반 AI 개발 방식은 크게 ① 서비스형 LLM(상용 AI 서비스) 활용, ② 기성 LLM(공개 모델) 활용, ③ 자체개발 방식으로 구분될 수 있는데, 공통적으로 개인정보 안심설계 원칙(Privacy by Design; PbD)을 반영하여야 하고, 특히 대규모 또는 민감한 개인정보 처리가 수반되는 경우 개인정보 영향평가가 권장됩니다.
  특히, 생성형 AI 개발·운영 과정에서 개인정보 영향평가를 실시하는 경우, 기존 제도·절차를 활용하되 ① 개인정보 흐름 분석 단계(학습데이터 수집부터 학습, 추론, 출력 생성에 이르는 AI 데이터 처리 과정 전반의 개인정보 처리 현황을 체계적으로 파악), ② 침해요인 분석 단계(전통적인 개인정보 침해 외에도 생성형 AI 관련 새로운 프라이버시 리스크를 분석), ③ 개선계획 수립 단계(생성형 AI의 혁신성과 개인정보 보호를 동시에 확보할 수 있는 실효성 있는 방안 마련) 별 검토가 권장됩니다.

(3) AI 학습 및 개발

- 생성형 AI는 기술적 특성으로 인해 원본 정보가 그대로 출력되거나 민감정보가 추론 목적으로 운용되는 등 정보주체의 권익 침해 가능성이 존재하므로, 학습 및 개발 단계에서부터 다음과 같은 주요 프라이버시 사항들을 고려하여야 합니다.

수준	주요 고려사항
데이터 수준	• 데이터 오염, 데이터 편향성부정확성 등 문제 대응 • 공개 데이터 수집 시 명시적인 스크래핑 거부 의사를 표시한 콘텐츠 제외 • AI 학습 전 민감한 정보의 삭제 또는 가명익명화
모델 수준	• 미세조정 및 정렬 기법을 활용한 추가 안전조치 확보 • 적대적 공격에 대응하기 위한 기술적 조치 적용
시스템 수준	• 외부 API 연동 시 접근제어 통한 보호 체계 구축 • 입·출력 단계에서의 필터 활용 • RAG 등 외부 DB 활용 시 추가적인 안전조치 적용

(4) 시스템 적용 및 관리

- 개발 완료 이후 단계에서도 프라이버시 관련 요소들에 대한 고려가 필요합니다. 시스템 배포 전에는 실제 동작 환경에서 AI의 정확도, 안정성을 평가하여 프라이버시 리스크를 점검해야 하며, 배포시에는 이용자들이 지켜야 할 '허용되는 이용방침'(AUP, acceptable use policy) 등을 작성공개함으로써 배포 후 오남용을 방지하는 것도 필요합니다.
- 시스템 배포 이후에는 신고의견 제출 기능을 제공함으로써 부적절한 결과물에 대응하고, 자동화된 결정에 대한 거부권이나 설명 및 검토요구권 등 개인정보 보호법에 따른 정보주체의 권리행사에 성실하게 대응하여야 합니다. 이를 위해서는 개인정보 처리방침, FAQ 등을 통해 AI 시스템의 개인정보 처리 과정을 투명하게 공개할 것이 권장됩니다.

3. AI 프라이버시 거버넌스 체계

- 생성형 AI의 데이터 처리 흐름이 복잡해짐에 따라 개인정보 관련 법규 준수를 위해 개인정보 보호책임자(CPO)를 중심으로 내부 관리체계를 구축운영할 필요가 있습니다.
- 구체적으로 ① 생성형 AI 활용 전 과정에 대한 개인정보 처리의 적법성 및 안전성 확보를 위해 CPO가 관리감독 책임을 수행할 수 있는 체계 구축, ② 개인정보 영향평가, 레드티밍 등을 활용한 지속적인 생성형 AI 프라이버시 리스크 평가, ③ 최고인공지능책임자

(CAIO), 정보보호최고책임자(CISO) 등과의 긴밀한 협력 체계를 유지, ④ AI 기획개발 초기 단계부터 개인정보 안심설계(PbD) 관점의 서비스 내재화가 필요합니다.

4. 시사점

본 안내서는 생성형 AI 개발활용 전 단계에 걸쳐서 단순히 개인정보보호법 준수에 필요한 사항뿐만 아니라 적극적인 프라이버시 보호를 위해 필요한 사항들까지 상세하게 안내하고 있습니다. 따라서 생성형 AI를 개발하거나 활용하고자 하는 기업 및 기관은 본건 안내서를 통해 안전한 프라이버시 관리 체계를 마련할 수 있을 것입니다.

본 안내서에 따른 생성형 AI 개발 및 활용 단계별 유의사항은 서로 유기적으로 연결되어 있기에 전 단계를 통합하여 하나의 체계 하에서 관리가 이루어질 필요가 있으며, 이를 위해서는 체계적인 AI 프라이버시 거버넌스 체계 구축과 개인정보 보호책임자(CPO)의 권한 및 역할의 재정립이 요구됩니다. 즉, 생성형 AI의 안전한 활용을 위해서는 회사의 프라이버시 거버넌스 체계를 새로 구축하거나, 기존 체계 전반을 면밀히 점검할 필요가 있습니다. 특히, 시행을 앞두고 있는 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」에서도 AI의 신뢰성·안전성 확보를 위한 관리체계 구축에 관한 규정을 두고 있는 점을 고려하면, 이러한 거버넌스 체계의 중요성은 더욱 크다고 할 것입니다.

AI 기술이 급속히 발전하는 만큼, AI 개발 및 활용과 관련하여 개인정보 및 프라이버시 보호를 포함한 다양한 법적 리스크에 대한 우려 또한 증가하고 있습니다. 생성형 AI를 활용하려는 기업 및 기관으로서는 향후에도 본 안내서를 포함하여 AI 및 개인정보 처리에 관한 법령, 안내서, 제도 등을 꾸준하게 모니터링할 필요가 있을 것입니다.

[English version] PIPC Issues Guidelines on the Processing of Personal Information for the Development and Use of Generative AI

관련구성원

강신욱
대표변호사

02-316-4059
sokang@shinkim.com

안정호
변호사

02-316-2891
jhahn@shinkim.com

장준영
변호사

02-316-4985
jyojang@shinkim.com

윤호상
변호사

02-316-2584
hsyoon@shinkim.com

김근호
변호사

02-316-1926
kehkim@shinkim.com
