SHIN&KIM
법무법인(유) 세종

개인정보보호위원회, 「AI 프라이버시 리스크 관리모델」 제시

2024.12.27

개인정보보호위원회는 2024년 12월 19일 **AI 기술을 도입, 적용**하면서 프라이버시 관련 **내부 관리체계를 마련, 정립, 정비하고자 하는 기업·기관** 등을 대상으로 **AI 프라이버시 리스크 관리**의 **방향과 원칙을 제시**하는 「AI 프라이버시 리스크 관리모델」을 공개하였습니다. 본건 모델에서는 AI 프라이버시 리스크의 관리 절차, 구체적인 리스크 식별·경감 방안 및 AI 프라이버시 리스크 관리 체계를 안내하고 있으며 그 주요 내용은 아래와 같습니다.

1. 주요 내용

(1) 본건 모델의 적용 범위

- **(적용 대상) AI 모델·시스템**(이하 "AI 서비스") **개발자**는 AI 데이터 처리의 목적, 범위, 수단 등을 결정하고, 개발 이후 발생할 수 있는 리스크를 예측·통제할 일정한 책임을 부담한다는 점에서, **AI 서비스 제공자**는 개발 완료된 AI가 정보주체의 권리의무에 영향을 미치는 결정 등을 출력하는 단계의 리스크를 예측하고 통제할 일정한 책임을 부담한다는 점에서 본건 모델을 참고 가능함
- **(리스크의 범위)** AI 서비스의 개발 및 제공 과정에서 파생될 수 있는 리스크 중 **프라이버시 측면**에서 국내외에서 중점적으로 논의되고 있는 리스크를 상정
- **(개인정보 보호법 및 타 안내서와의 관계)** 법령 및 개인정보보호위원회가 발간한 다른 안내서 내 준수사항을 AI 서비스에 그대로 적용하기는 어려우나, 본건 모델을 참고하고 해당 규정 및 기존 안내서 내용의 취지·목적을 고려하여 각 서비스에 적합한 조치가 무엇인지 판단하고 이를 수행할 필요가 있음

(2) AI 프라이버시 리스크의 관리 절차

- **(리스크 관리의 시점)** 리스크 관리는 리스크의 조기 발견 및 완화를 위해 **기획·개발 단계부터** 이루어지는 것이 바람직하며, 이후에도 AI 기술의 보강이 지속될 수 있고, 의도하지 않은 용례로 사용되거나 침해 환경이 악화되는 등 외부 요인이 변화할 수 있으므로 **주기적·반복적 위험 관리**가 권장됨
- **(세부 절차)** 리스크 관리 절차는 **(1) AI 유형·용례 파악, (2) 리스크 식별(mapping), (3) 리스크 측정(measuring), (4) 경감방안 검토·도입(mitigation)**으로 이어지는 4단계 절차가 권장됨

(1) AI 유형·용례 파악		(2) 리스크 식별		(3) 리스크 측정		(4) 경감방안 검토·도입
AI 서비스의 목적, 범위 등 구체적 맥락 파악	▶	파악된 유형 및 용례에 따라 발생 가능한 리스크 식별	▶	리스크 발생확률, 중대성, 수용가능성, 우선순위 등 판단	▶	리스크 경감을 위한 관리적, 기술적 방안 검토 및 실행

(3) 리스크 식별 방안

- **(기획·개발 단계)** AI 서비스 기획·개발 단계에서는 **PbD(Privacy by Design)* 원칙**을 기반으로 AI의 전체 생애주기에 걸친 리스크 관리체계의 토대를 마련할 필요가 있음
  * Privacy by Design: 제품·서비스 개발 시 기획 단계부터 개인정보 처리의 전체 생애주기에 걸쳐 이용자의 프라이버시를 고려한 기술·정책을 설계에 반영하는 것을 의미함 AI 학습데이터에 개인정보가 포함된 경우 **학습데이터의 수집 및 이용**은 개인정보처리에 해당하므로 AI 서비스 개발자는 AI 모델의 학습 단계부터 리스크를 관리할 필요가 있음오픈소스, API 형태의 타사 AI 모델을 활용하는 경우 기획 단계부터 **사업자간 책임분배** 등을 사전 검토할 필요가 있음
- **(서비스 제공 단계)** AI 서비스가 이용자로부터 데이터를 입력받아 합성콘텐츠, 평가·분류 결과 등 AI 추론 결과를 출력하는 과정에서 **정보주체의 권리침해**가 현실화될 수 있음 다만, **AI 서비스의 목적 및 출력 결과**에 따라 상이한 프라이버시 리스크를 가지므로 **개별적 검토가** 필요AI 서비스는 배포 이후에도 추가 학습, 기능 업데이트 등을 통해 지속적으로 수정·보완될 수 있으므로 학습데이터 수집·이용의 적법성 확보 등 **기획·개발 단계에서 검토한 리스크를 재검토**하는 등의 노력이 필요
- **(리스크 유형)** 개인정보위는 아래와 같이 **AI 생애주기 및 용례별 리스크**로서 대표적으로 고려될 수 있는 사안을 안내함

구분			일반 리스크	프라이버시 리스크
기획·개발			▪ 권리 침해 (저작권, 개인정보, DB권)	▪ 적법하지 않은 학습데이터 수집·이용 ▪ AI 학습데이터의 부적절한 보관·관리 ▪ AI 가치망의 다양화에 따른 데이터흐름 및 정보주체 권리보장 책임 복잡화
서비스 제공	생성 AI		▪ AI 합성 콘텐츠 오용 ▪ 권리 침해 ▪ 안보, 보안 문제	▪ 학습데이터 암기 및 개인정보 유·노출 ▪ 악의적 AI 합성콘텐츠로 인한 정보주체 권리 침해
	판별 AI	사람의 평가/분류	▪ 편향, 차별, 품질 편차 ▪ 불투명성	▪ 학습데이터 암기 및 개인정보 유·노출 ▪ 자동화된 결정으로 인한 정보주체 권리 약화
		추천 시스템	▪ 프로파일링, 정치적 양극화	▪ 학습데이터 암기 및 개인정보 유·노출 ▪ 대중감시 및 민감정보 추론 위협
		사실의 인지	▪ 편향, 품질 편차	

(4) 리스크 경감 방안

- **(관리적 조치)** 개인정보위는 AI 프라이버시 리스크를 경감하기 위한 **관리적 조치**를 아래와 같이 제시함

  - ① 학습데이터 출처·이력 관리
  - ② 안전한 보관·파기 방안 마련 및 실행
  - ③ AI 가치망 참여자간 역할 명확화(처리위탁, 국외이전 등 발생시)
  - ④ 허용되는 이용 방침(acceptable use policy; AUP)의 작성, 공개
  - ⑤ AI 프라이버시 레드팀 구성·운영
  - ⑥ 정보주체 신고 방안 및 조치 방안 마련
  - ⑦ 자동화된 결정에 대한 개인정보처리자의 조치 기준 준수(거부권, 설명 요구권, 검토 요구권 보장 등)
  - ⑧ 개인정보 영향평가 수행 고려

- **(기술적 조치)** 개인정보위는 AI 프라이버시 리스크를 경감하기 위한 **기술적 조치**를 아래와 같이 제시함

  - ① 학습데이터 전처리(데이터 최소화, 가명·익명화, 중복제거 등)
  - ② AI모델 학습시 합성데이터 사용 고려
  - ③ 모델 미세조정을 통한 안전장치 추가
  - ④ 입력 및 출력 필터링 적용
  - ⑤ 차분 프라이버시 기법(특정 데이터베이스에 잡음을 추가하는 기법) 적용
  - ⑥ 출처 데이터 추적 및 합성콘텐츠 탐지 방안 마련
  - ⑦ 생체정보 활용시 가명·익명처리 기술 적용

(5) AI 프라이버시 리스크 관리 체계 구축 방안

- **(AI 프라이버시 거버넌스 구축)** AI 기업·기관 등은 AI 프라이버시 리스크 관리를 위해 **개인정보보호책임자(CPO) 중심의 내부 거버넌스 체계**를 정비·마련하는 것이 바람직함 조직의 사업적 요구사항뿐만 아니라 규제 및 사회적 요구사항을 종합적으로 이해하고 있는 CPO의 역할이 중요CPO 등을 중심으로 담당조직을 구성하여 적절한 부서 및 개인에게 권한과 책임을 부여해야 함본건 모델 등을 참고하여 AI 프라이버시 리스크를 평가·관리하는 정책을 마련해 문서화하고, 담당조직을 중심으로 이행하여야 함
- **(AI 가치망 내 참여자와의 협력)** AI 가치망의 다양한 참여자간 상호의존적 활동 안에서 **당해 기업·기관의 역할** 및 **타 기업·기관**과의 **협력체계**를 **구체화**하는 것이 바람직함 AI 서비스 개발 범위(직접 개발, 오픈소스 및 API 이용 등) 등을 기반으로 당해 기업·기관의 권한 또는 역할 등을 정의한 후 타 기업 및 기관과 협력체계를 구축할 필요

2. 시사점

- 개인정보보호위원회가 공개한 「AI 프라이버시 리스크 관리모델 」은 AI 프라이버시 리스크의 관리 절차와 함께 구체적인 리스크 식별 · 경감 방안 및 AI 프라이버시 리스크 관리 체계를 안내하고 있으며 나아가 AI 개인정보 리스크 자율평가 항목을 제시하고 있으므로, AI 기술을 도입, 적용하고자 하는 기업 및 기관은 본건 모델을 통해 AI 프라이버시 리스크 관련 내부 관리체계를 새로 마련 또는 정립하거나, 기존에 수립된 관리체계를 정비할 수 있을 것으로 보입니다.
- 특히, 본건 모델은 개별 AI 서비스에 개인정보 보호법이 적용될 수 있는 가능성을 안내하면서 CPO 및 담당조직의 중요성을 강조하고 있으므로, CPO 및 담당조직은 본건 모델을 참고하여 기획 또는 서비스 중인 AI 서비스의 각 생애주기별 프라이버시 리스크를 정책적, 법률적으로 면밀히 재검토할 필요가 있는 것으로 판단됩니다.
- 또한, 본건 모델은 최근 국회 법제사법위원회를 통과한 「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 제정안, 이른바 'AI 기

본법’에서도 인공지능사업자의 위험 식별, 평가 등 AI와 관련된 위험에 관한 전반적 관리방안 수립·운영 의무와도 밀접한 관련이 있는 만큼 AI와 관련된 제반 의무 이행 방안과 연계하여 면밀히 살펴볼 필요가 있을 것입니다.

About Shin & Kim’s ICT Group

법무법인(유) 세종은 다양한 산업 간 융합과 혁신이 창출되는 ICT 분야에 차별화된 전문성과 인적 네트워크(윤종인 전 개인정보보호위원회 위원장, 김영호 전 행정안전부 차관, 최재유 전 과학기술정보통신부 차관 등)를 보유하고 있으며, AI센터에서도 AI 등 신기술을 활용하는 기업들의 법 위반 리스크 및 비즈니스 리스크 최소화를 위한 전문적인 자문을 제공하고 있습니다. 특히, 최근 발간된 개인정보보호위원회 · 한국개인정보보호책임자협회(KCPO)의 CPO 핸드북의 감수 및 집필에 참여하는 등 조직 내 개인정보 거버넌스 구축에 전문성을 보유하고 있습니다. AI를 포함한 ICT 산업 전반에 대한 규제 동향 파악 및 대관, 입법컨설팅, 규제 영향력 분석과 기업의 전략 수립 등에 대한 법률자문을 제공하고 있으므로, 보다 전문적인 내용이나 궁금하신 사항이 있으면 언제든지 연락 주시기 바랍니다.

관련구성원

장준영
변호사

02-316-4985
jyojang@shinkim.com

윤호상
변호사

02-316-2584
hsyoon@shinkim.com

정영운
변호사

02-316-1822
ygjeong@shinkim.com

이지은
선임연구위원

02-316-1720
jeunlee@shinkim.com