SHIN&KIM
법무법인(유) 세종

AI 시대 안전한 개인정보 활용 정책방향 발표

2023.08.08

개인정보보호위원회는 8월 3일 「인공지능 시대 안전한 개인정보 활용 정책 방향」을 발표하였습니다. AI에 대한 기대와 우려 사이에서 프라이버시 침해 위험은 최소화하면서 AI 혁신 생태계 발전에 꼭 필요한 데이터는 안전하게 활용할 수 있도록 정책방향을 수립하였습니다.

주요내용은 (i) AI 프라이버시팀 신설(10월 중), (ii) 기획-데이터수집-AI학습-서비스 단계별 AI 처리기준 구체화 (iii) AI 프라이버시 민관 정책협의회를 신설하여 가이드라인 마련, (iv) 국제적 공조체계 강화로, 아래에서 더 자세히 살펴보도록 하겠습니다.

이번에 발표한 정책방향은 현 시점에서의 기초적인 기준과 원칙이며, 개인정보보호위원회는 향후 학계·산업계·시민 단체 등 의견을 충분히 수렴하여 이를 구체화해 나갈 계획입니다.

주요 추진과제

1. 불확실성 해소를 위한 원칙 기반 규율 추진체계 정립

> 변화 속도가 빠르고 데이터 활용 범위, 방식이 고도로 복잡한 AI에 대해 그 특성을 고려하여 규정 중심이 아닌 원칙(principle) 중심의 규율체계를 정립

- 이를 위해 AI 관련 사항을 전담하는 **‘(가칭) AI 프라이버시팀’을 10월 중 신설** ‘AI 프라이버시팀’에서는 AI 모델·서비스를 개발·제공하는 사업자와 소통창구를 마련하여 개인정보 처리의 적법성, 안전성 등에 대한 **법령해석을 지원**하거나 **규제 샌드박스[1] 적용을 검토**하는 등 적극적인 컨설팅 역할을 수행하여 불확실성을 축소
- 또한 **‘(가칭)사전 적정성 검토제’도 올해 중 도입** 사업자 요청 시 비즈니스 환경을 분석하여 「개인정보 보호법」을 준수할 수 있도록 적용방안을 함께 마련하고, 이에 따른 사업자의 이행결과에 대해 **개인정보보호위원회가 적정하다고 판단한 사안에 대해서는 행정처분을 하지 않는 제도**미국 금융·공정거래 등의 분야에서 널리 활용하고 있는 ’No Action Letter‘, 그리고 유럽연합 GDPR의 ‘사전 협의’(prior consultation) 제도로부터 시사점을 얻어 새롭게 구상한 제도임

2. AI 개발·서비스 단계별 개인정보 처리기준 구체화

현행 「개인정보 보호법」 체계 하에서 그간의 해석례·의결례·판례 등을 종합하여 AI 개발·서비스 기획-데이터 수집-AI 학습-서비스 제공 등 단계별로 개인정보를 어떠한 원칙과 기준에 입각하여 처리할 수 있는지에 대해 최대한 구체화하여 발표

다만 이번에 발표한 정책방향은 **현 시점에서의 기초적인 기준과 원칙** 이며, 향후 학계·산업계·시민 단체 등의 **의견을 충분히 수렴하여 구체화해 나갈 계획**

- **기획·설계 단계:** 개인정보보호 중심 설계(Privacy by Design) 원칙 반영
- **데이터 수집 단계**

- 1) 일반 개인정보 계약 체결·이행, 법령 준수, 정보주체 동의 등에 따라 적법하게 수집한 개인정보는 '수집 목적 범위 내'에서 AI 개발·서비스를 위해 이용 가능AI 개발·서비스가 ① 당초 수집 목적과 합리적으로 관련된 범위에서 ②예측 가능하고 ③정보주체의 이익을 부당하게 침해하지 않으며 ④안전성 확보에 필요한 조치를 한 경우 추가적 이용 가능

(참고) 추가적 이용이 가능한 사례(예시)

특정 서비스 제공 목적으로 수집한 개인정보를 해당 서비스의 개선(고도화) 목적 으로 AI 개발에 이용하는 것은 당초 수집 목적과 합리적 관련성이 있고 정보주체 이익을 부당하게 침해할 가능성이 낮으므로 추가적 동의 없이 이용·제공 가능

■ **(후속과제)** AI 학습방법, 서비스 기능 등을 고려하여 AI 개발·서비스에 적용할 수 있는 '합리적으로 관련된 범위'의 판단 기준 구체화

- 2) 공개된 정보 공개된 정보의 처리에 대한 이익 형량 결과, 처리 시 얻을 수 있는 이익이 이를 막음으로써 얻는 이익보다 크다고 인정되는 경우, ① AI 개발·서비스가 정보주체의 동의의사가 있었다고 객관적으로 추단되는 범위 또는 ② AI 개발·서비스를 제공하는 개인정보처리자의 정당한 이익이 정보주체의 권리보다 명백히 우선하는 범위 내에서 수집·이용 가능

(참고) 공개된 정보 처리 관련 이익 형량 시 고려사항

- ◦ 민감정보 처리제한(§23), 노출된 개인정보의 삭제·차단(§34의2) 등을 준수할 것
- ◦ 웹사이트 운영자가 'robots.txt' 설정을 통해 로봇의 접근을 제한한 경우 해당 페이지에는 접근하지 않는 로봇배제표준을 준수할 것
- ◦ 시간 · 비용 · 기술을 합리적으로 고려하여 특정 개인을 식별하기 어렵도록 하는 조치(계정정보 등 분리, 특정 개인을 식별할 수 있는 주민등록번호·운전면허번호·카드번호 등 식별자 삭제 등)의 이행여부 및 조치 수준
- ◦ 개인을 유추하거나 식별할 목적으로 데이터를 처리하는지 여부(공적인 인물에 관한 정보로서 알 권리가 중요하다고 판단되는 범위에 대해서는 정확성 · 최신성 확보를 위해 합리적으로 필요한 범위 내에서 식별 목적으로 처리 가능)
- ◦ 서비스 과정에서 개인정보 침해에 대한 모니터링을 실시하고 정보주체에게 대응 수단을 제공하며, 침해 발생 시 즉시 조치할 수 있는 체계를 갖추었는지 여부
- ◦ 학습데이터 출처, 개인정보 처리방법 등을 투명하게 공개하는지 여부

(참고) 동의 의사의 객관적 추단 시 고려사항

- ◦ 공개된 개인정보의 성격, 공개 형태 및 대상 범위

◦ 추단되는 정보주체의 공개 의도
◦ 정보처리자의 정보제공 등 처리의 형태와 그 정보제공으로 인하여 공개의 대상 범위가 원래의 것과 달라졌는지 여부
◦ 원래의 공개 목적과 상당한 관련성이 있는지 여부

■ **(후속과제)** '정당한 이익'의 구체적 내용, 개인정보처리자의 정당한 이익이 인정되는 사례 등 처리자가 참고할 수 있는 가이드라인 마련

◦ 공개된 정보를 크롤링으로 수집, 가명처리 후 AI 학습에 이용 가능

- 3) 영상정보 **고정형 기기:** 당초 설치·운영 목적(범죄예방, 시설안전 등)과 관련된 AI 개발 등에 CCTV 영상 이용 가능. 관련 없는 경우 익명·가명처리 필요. 얼굴인식 등 개인의 특징점을 추출하는 AI개발은 사전 동의 또는 법령상 근거 필요**이동형 기기:** 당초 촬영목적 달성을 위해 필요한 범위 내에서 안전조치(전송구간 암호화, 접근통제 등) 후에 원격 관제, 최소한의 저장 가능

■ **(후속과제)** 불특정 다수 영상은 익명·가명처리가 필요하나, 익명·가명 데이터를 통해서는 AI 품질 확보가 어려운 경우를 고려하여 규제샌드박스 등을 통해 강화된 안전조치(인적 개입 차단, 지속·주기적 점검 등 관리체계 마련, 책임성 강화 등) 하에 원본 활용 검토

- 4) 생체인식정보 별도 동의가 있거나 법령 근거가 있는 경우에만 처리가능. 크롤링 등을 통해 공개된 정보에서 생체인식 정보를 추출하여 수집하거나 생성·처리하는 것은 엄격히 제한생체인식정보 처리 시 대체수단마련, 원본정보 분리 보관 등 보호조치 이행

■ **(후속과제)** 생체인식정보는 특수성(유일성, 불변성)과 해외 입법례 등을 고려하여 별도 법 체계 마련 추진

- **AI 학습 단계**

◦ 과학적 연구 등의 목적으로 가명처리하여 동의없이 AI 개발 가능. 다만, 이 경우에도 다른 정보와의 연계·결합을 통한 재식별 등 사전·사후적으로 발생 가능한 위험에 대한 방지 조치가 중요하다는 점을 강조

■ **(후속과제)** 이미지, 영상, 음성, 텍스트 정보 등 비정형데이터의 가명처리 원칙, 식별 위험성 점검기준, 데이터 항목별 가명처리 방법, 관련 가명처리 기법·사례 등 구체적 기준 마련 추진

◦ 활용목적·처리환경에 맞는 개인정보보호 강화기술(Privacy Enhancing Technology, PET) 활용

■ **(후속과제)** 합성데이터(synthetic data[2])를 안전하게 생성하여 AI 학습 등에 활용할 수 있도록 관련 절차 및 권고기준 마련

■ **(후속과제)** PET 적용이 모호하거나 검증이 필요한 경우, 보안성·안전성이 확보된 공간에서 기술개발·실증이 가능하도록 제도 마련

■ **(후속과제)** AI 학습용 데이터 생성·검증 기술, AI에 대응한 프라이버시 보호 기술개발 등 R&D 확대

- **서비스제공 단계** AI 학습데이터 수집 방법, 서비스 과정에서 생성되는 정보의 처리방법 등 안내**(후속과제)** 구체적인 공개범위·내용, 고지방안 등에 대한 명확한 기준 및 '설명 가능한 AI(explainable AI)'를 위한 AI 설명내용·방법 등 구체화

◦ 삭제·처리정지·자동화된 결정 대응권 등 정보주체 권리행사 보장

■ **(후속과제)** 자동화된 결정에 대한 거부권·설명요구권 등 정보주체 권리행사 보장방안, 데이터 오류 등에 대응할 수 있는 방법 등 구체화

◦ 파운데이션 모델 등 기존 AI 모델의 API를 활용하거나, 기존 서비스에 플러그인을 추가하는 경우에도 안전조치 필요
◦ - 개인정보 보호 제도·절차, 기술적 안전조치 등을 갖춘 신뢰성 높은 기업만 API 사용 또는 플러그인을 추가할 수 있도록 절

차 마련 필요

- ❍ - API 사용자·플러그인 개발자가 개인정보 보호 조치를 준수할 수 있도록 상세한 사용지침, 기술문서 등을 제공하고, 준수여부에 대한 지속 모니터링 필요

3. 민관협력을 통한 분야별 가이드라인 마련

- AI 기업·개발자, 학계·법조계, 시민단체 등 민·관이 함께 논의할 수 있는 'AI 프라이버시 민·관 정책 협의회'를 오는 10월 중 구성하여 실제 현장에서 적용할 수 있는 가이드라인 마련 예정

[주요 과제 추진계획(안)]

구분	내용	시기
비정형데이터 가명처리 기준	이미지·영상, 음성 등 비정형데이터의 가명 처리 기법·사례, 식별위험성 점검기준 등	'23.12월
생체인식정보 규율체계	실시간 원격 얼굴인식 기술 제한기준, 영향 평가 의무 대상 생체정보 기준 등	'23.12월(법안마련)~'25년(입법추진)
공개된 정보 활용 가이드라인	공개된 정보 활용 시 '정당한 이익'(법 §15①6.), '추가적 이용'(법 §15③) 등 판단기준 및 사례	'24.3월
이동형 영상기기 촬영정보 활용 가이드라인	이동형 영상기기로 인한 '부당한 권리침해'의 판단기준 구체화 및 사례 제시	'24.6월
AI 투명성 확보 가이드라인	학습데이터 출처 및 수집방법의 공개 수준, 열람·삭제·처리정지권 등 권리 행사 방법 등	'24.6월
합성데이터 활용 가이드라인	AI 활용을 위한 합성데이터 생성·처리기준	'24.9월

4. AI 글로벌 협력체계 공고화

- 지난 6월 서울에서 개최한 「AI와 데이터 프라이버시 국제 컨퍼런스」를 시작으로 주요국 개인정보 감독기구와 함께 각 나라의 법·정책, 처분 사례 등을 공유
- 2025년 글로벌 프라이버시 총회(Global Privacy Assembly, GPA)를 유치하여 AI를 중심으로 디지털 심화 시대에 새롭게 대두되는 프라이버시 이슈에 대해 논의
- 오픈AI, 구글, 메타 등 글로벌 AI 사업자 및 국내 AI 사업자와의 소통도 활성화

시사점

- 이번 AI 정책방향은 인공지능 기술을 활용하는 기업들에게 현행 개인정보 보호법 체계 하에서의 일응의 데이터 처리 기준을 제시하고 있습니다.
- 구체적인 세부내용은 향후 민관 정책 협의회에서 논의될 것으로 보이는바, 향후 관련 가이드라인 논의 및 내용이 구체화되는 과정을

주목할 필요가 있습니다.

[1] 기존 규제에도 불구하고 신기술·신산업 시도가 가능하도록 일정 조건(시간, 장소, 규모) 하에서 규제를 면제·유예해주는 제도
[2] 원본 데이터의 통계적 특성을 추출·학습하여, 실제 원본 데이터 분석 결과와 유사한 결과를 얻을 수 있도록 가상으로 재현한 데이터

관련구성원

강신욱
대표변호사

02-316-4059
sokang@shinkim.com

안정호
변호사

02-316-2891
jhahn@shinkim.com

황정현
변호사

02-316-1775
jhhwang@shinkim.com

윤호상
변호사

02-316-2584
hsyoon@shinkim.com

강지현
변호사

02-316-1518
jhykang@shinkim.com