2024. 7. 17.(수) 14:00
정부서울청사 3층 브리핑룸

# 『AI 개발·서비스를 위한 공개된 개인정보 처리 안내서』

# 브리핑문

개인정보보호위원회

# Ⅰ. 추진 경과

안녕하십니까?

개인정보보호위원회 개인정보정책국장 양청삼입니다.

바쁘신 가운데도 브리핑에 참석해주신

기자님들께 감사의 인사를 드립니다.

개인정보위는 사회 전 부문에서

**인공지능과 디지털 시대로의 전환**이 가속화됨에 따라

작년 8월 「**AI시대 안전한 개인정보 활용 정책방향**」을 발표하고,

**AI 산업의 혁신과 발전, 인공지능·데이터 처리**에 대한

**국민의 신뢰**를 확보하기 위해 노력해 왔습니다.

지난 2월 발표된 **비정형데이터 가명처리 기준,**

5월 발표된 「**합성데이터 생성 참조모델**」에 이어

**3번째**로 발표하는 이번

「**AI 개발·서비스를 위한 공개된 개인정보 처리 안내서**」는

빠르게 변화하고 있는 **인공지능·데이터 처리 환경**에 적용할 수 있는

**개인정보 보호 원칙**과 **기준**을 **구체화**한 것으로서,

**대규모 언어모델(LLM)** 등 AI 개발에 **'핵심원료'**인

**공개된 개인정보**가 **적법**하고 **안전**하게 활용될 수 있도록

일정한 **기준**을 제시함으로써 **기업 불확실성**을 낮추고

**국민 신뢰**를 높이기 위한 취지에서 준비되었습니다.

이번 안내서는 학계, 산업계, 시민단체 등 **AI 분야 차세대 전문가**가 참여하는 「**AI 프라이버시 민·관 정책협의회**」가 주축이 되어 마련되었고,
**각계의 광범위한 의견수렴**을 거쳐 최종 확정되었습니다.

## Ⅱ. 안내서 마련 배경

현재 우리가 일상에서 유용하게 사용하고 있는
**ChatGPT, 하이퍼클로바X** 등 국내외 주요 AI 모델은
방대한 데이터를 학습한 결과물이며,
주로 **위키백과**(wikipedia), **블로그, 커먼 크롤**(common crawl) 등
다양한 웹사이트에 공개된 데이터가 학습에 이용되고 있습니다.

이러한 공개 데이터에는 **주소, 이메일, 고유식별정보** 등
**다양한 개인정보**가 **포함**될 수 있어
국민의 프라이버시 침해 없이
**안전하게 활용**하기 위한 **기준**이 필요하나,

**현행 법제**에는 공개된 개인정보를 처리할 수 있는
**명시적 기준이 없어 기업 불확실성**이 높은 상황입니다.

이에, 개인정보위는 이번 안내서를 통해
**AI 개발 및 서비스**를 위해 **공개된 개인정보**를
**적법하게 활용**할 수 있는 **법적근거**를 명확히 안내하고,
AI 기업이 이행할 수 있는 **다양한 안전조치**를
**'AI 학습-서비스' 주기별**로 안내하였습니다.

최근 **미국**과 **유럽연합(EU) 주요국**에서도
공개 데이터를 포함한 **AI·데이터 처리 전반**에 대한
**개인정보 규율체계**를 **형성**하고 있어,
**글로벌 상호운용성 확보** 측면도 적극적으로 고려하였습니다.

## Ⅲ. 안내서 주요 내용

### ❶ 먼저, AI 개발을 위해 공개된 개인정보가 수집·이용될 수 있는 개인정보 보호법상의 근거로서 '정당한 이익' 적용 기준·요건을 구체화하였습니다.

**공개된 개인정보**는 개인정보처리자와 정보주체 간에
**특정 서비스**를 **매개**로 연결되는 **직접적 관계**가 없어
**개별 동의**나 **계약 체결** 등의 근거 적용이 **사실상 어려웠습니다.**

이에, **AI 개발 목적**과 **공개된 개인정보의 특성**,
**리스크 수준** 등을 고려하여
개인정보처리자 이익과 정보주체 권리를 **비교형량**하는
**'정당한 이익'** 조항이 **실질적인 적법근거**가 될 수 있다고 판단하고,
해당 조항을 원용할 수 있는 **기준·요건**을 **구체화**하였습니다.

**정당한 이익 성립 요건**은 크게 **3가지**로,
첫 번째 요건은 ❶**목적의 정당성**입니다.
AI 기업은 공개된 개인정보 처리를 통해 개발하려는
**AI의 목적·용도**를 **구체화**하여 정당한 이익이 있음을
주장할 수 있습니다.

두 번째 요건은 ❷**처리의 필요성**입니다.
AI 개발·서비스에 **공개된 개인정보 처리의 필요성**과
**상당성·합리성**이 인정되어야 합니다.

예컨대, **의료진단보조 AI**를 개발하는 경우,
**개인의 소득·재산** 등 AI 목적과 관련 없는 정보는
**학습데이터에서 배제**해야 합니다.

마지막 요건은 ❸**구체적 이익형량**입니다.
개인정보처리자의 **정당한 이익**이 **정보주체 권리**에
**명백히 우선**하는지를 평가해야 합니다.

이때, AI 기업은 안내서에 제시된 **안전성 확보조치** 및
**정보주체 권리보장 방안**을 적절히 도입하여
**프라이버시 침해 위험을 낮출 수 있습니다.**

## ❷ 다음으로 AI 기업이 이행할 수 있는 최소한의 안전성 확보조치 기준과 정보주체 권리보장 방안에 대해 말씀드리겠습니다.

안내서는 **빠른 기술변화**를 고려하여
**AI 기업이 유연하게 도입·시행**할 수 있는
다양한 **기술적·관리적 안전조치**를 안내하였습니다.

AI 기업은 **기술적 조치**의 일환으로
▲**학습데이터 수집 출처의 적법성 검증**,
▲**개인정보 유·노출 방지 조치**,
▲**미세조정을 통한 안전장치 추가**,
▲**프롬프트 및 출력 필터링 적용** 등을 고려할 수 있고,

**관리적 조치**로서
▲**학습데이터 수집·이용 기준 정립·공개**,
▲**'(가칭)AI 프라이버시 레드팀' 구성·운영**
▲**개인정보 영향평가 수행** 등을 고려할 수 있습니다.

안내서에 제시된 **모든 조치의 이행**이 **요구되는 것은 아니며**,
AI 기업은 **개별 조치의 장·단점**,
**편향·차별 등 부작용, 성능저하 관계** 등을 고려하여
**「안전조치의 최적 조합」**을 **자율적**으로 **선택**하여 **이행**할 수 있습니다.

지난 3월 발표한 **주요 LLM 서비스 사전 실태점검 결과**를 보면,
AI 기업들이 도입한 **안전성 확보조치의 방식·수준**은 다양했습니다.

**AI 학습 단계**에서 특정범주의 개인정보를 **비식별화**하는
**사전조치**에 중점을 둔 기업도 있는 반면,
**AI 서비스 단계**에서의 **사후 필터 조치**에 중점을 둔 기업도 있었습니다.

이러한 여러 안전조치를 **종합적으로 검토**한 결과,
**각 조치들이 갖는 장·단점**이 있고 **기술변화 속도**도 빠르기 때문에
**일의적**으로 **특정한 조치**들을 정해서 권고하기 보다는,
각 기업이 자신들의 **AI 모델의 특성, 학습데이터 출처** 등을 고려해서
**안전조치의 최적 조합**을 정할 수 있도록 한 것입니다.

다만, AI 기업이 **「최적 조합」**을 선택하는데 참고할 수 있도록
**주요 LLM 기업**의 **실제 안전조치 이행사례**를
종합적으로 안내하였습니다.
아울러, **AI 환경에서 약화**될 수 있는 **정보주체 권리**를 보완하여
AI 기업이 이행할 수 있는 **권리보장 방안**을 **제시**하였습니다.

정보주체 알권리 보장을 위해 공개된 개인정보 수집사실과
주요 수집출처 등을 개인정보 처리방침 등에 안내하고,

실제 정보주체 권리 침해가 발생할 경우에는
합리적 범위 내에서 개인정보 삭제·처리정지 등
신속한 구제방안을 마련하여 지원토록 하였습니다.

❸ **마지막으로, 책임있는 AI 개발·활용을 위한 AI 기업의 역할을 제시했습니다.**

AI 기업은 개인정보보호책임자(CPO)를 구심점으로 하는
'(가칭)AI 프라이버시 담당조직'을 자율적으로 구성·운영하고,
안내서에 따른 기준 충족 여부를 평가하여
그 근거를 작성·보관하는 것이 바람직합니다.

또한, AI 성능 개선 등 중대한 기술적 변경이나
개인정보 관련 리스크 요인을 주기적으로 모니터링하고,
개인정보 침해사고 발생 시
신속한 권리 구제 방안을 제공해야 합니다.

## Ⅳ. 마무리 말씀

이번 안내서는 현시점의 해석 기준을 제시한 것으로서
향후 기술발전 추이, 관련 법령 제·개정, 해외 동향 등을
참고해 지속 업데이트될 예정입니다.

또한, 사전적정성 검토제, 규제샌드박스 등
다양한 혁신지원제도를 통해

**AI 기업, 국민**과 수시로 **소통**하면서 **개선사항**을 **발굴**하는 한편, 곧 출범하는 「**국가인공지능위원회**」를 통해
**AI·데이터 프라이버시 정책**을 **정교화**해 나가겠습니다.

추가로 설명이 필요한 부분은 질의응답을 통해
보다 상세히 설명해 드리도록 하겠습니다. 감사합니다.