개인정보보호위원회 보도자료 다시 대한민국! 새로운 국민의 나라

보도시점 2023. 8. 3.(목) 10:00 배포 2023. 8. 2.(수) 16:00

신뢰 기반 인공지능 데이터 규범, 첫 발 떼다

- 개인정보위, 「인공지능 시대 안전한 개인정보 활용 정책방향」 발표
- AI 단계별 개인정보 처리원칙 제시 · 신속한 법령해석 · 컨설팅 지원
- AI 개인정보 분야 글로벌 디지털 신질서 선도 추진

개인정보보호위원회(위원장 고학수, 이하 '개인정보위')는 8월 3일 정부서울청사에서 브리핑을 개최하고 **「인공지능 시대 안전한 개인정보 활용 정책방향」**을 발표하였다.

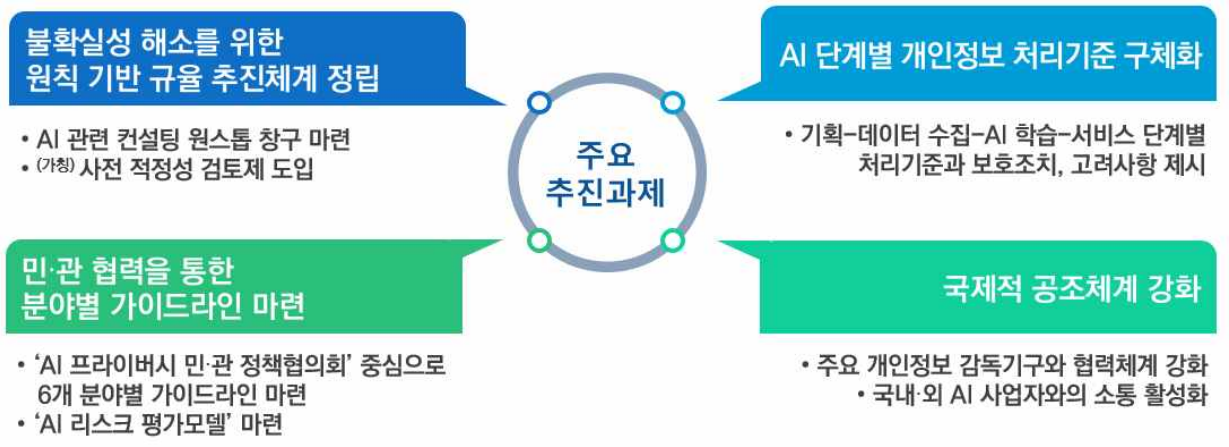
챗 GPT 등장 이후 의료, 교육, 유통 등 다양한 분야에서 인공지능(Artificial Intelligence, 이하 AI)을 활용한 서비스가 고도화되면서 AI가 가져오는 **편익에 대한 기대**가 높아지고 있다. 하지만 AI 기술의 중점이 대규모 언어 모델을 기반으로 한 **생성형 AI**[1]로 이동하고, 공개된 정보를 활용하거나 자율주행차·서비스 로봇 등으로 데이터를 수집하는 등 **정보주체가 예측하지 못한 방식**으로 데이터가 처리되는 경우가 증가하면서 **개인정보 침해 가능성에 대한 우려의 목소리** 역시 높아지고 있는 것이 사실이다.

개인정보위는 이러한 AI에 대한 기대와 우려 사이에서 **프라이버시 침해 위험은 최소화**하면서 **AI 혁신 생태계 발전에 꼭 필요한 데이터는 안전하게 활용**할 수 있도록 이번 정책방향을 수립하게 되었다. 특히, AI 환경에서 현행 「개인정보 보호법」을 어떻게 해석·적용할 수 있을지에 대한 **준칙을 제시**하는 한편, 구체적인 세부 사항에 대해서는 향후 정부와 민간이 협력하여 **규율체계를 공동 설계**해 나가는 청사진을 제시하는 데 중점을 두었다.

「인공지능 시대 안전한 개인정보 활용 정책방향」에 따라 개인정보위가 향후 중점적으로 추진해나갈 내용은 다음과 같다.

1) 생성형 AI(generative AI)는 사용자의 특정 요구(프롬프트)에 대응하여 텍스트, 이미지 등 결과를 만들어 내는 인공지능을 의미

[주요 추진과제]



1. 불확실성 해소를 위한 원칙 기반 규율 추진체계 정립

국내 AI 산업은 매출규모가 2020년 1.9조원에서 2022년 4조원 가까이 증가할 정도로 급속도로 성장하고 있으며, 그 쓰임새도 국민의 일상생활 뿐만 아니라 전문영역까지 다양해지고 있다. 해마다 AI 산업에 많은 기업들이 진입하고 있지만, 이들은 데이터를 수집하고 활용하는 데 있어 개인정보 보호 법령 등 관계 법령의 저촉여부를 둘러싸고 불확실성을 호소하고 있다.

개인정보위는 이렇듯 변화 속도가 빠르고 데이터 활용 범위, 방식이 고도로 복잡한 AI에 대해 그 특성을 고려하여 규정 중심이 아닌 **원칙(principle) 중심의 규율체계**를 정립해 나간다. 이를 위해 AI와 관련된 사항을 전담하는 원스톱 창구인 **'(가칭)AI 프라이버시팀'을 10월 중 신설**한다.

'(가칭)AI 프라이버시팀'에서는 AI 모델·서비스를 개발·제공하는 사업자와 소통창구를 마련하여 사안별로 개인정보 처리의 적법성, 안전성 등에 대한 **법령해석을 지원**하거나 **규제 샌드박스**[2] **적용**을 검토하는 등 **적극적인 컨설팅 역할**을 수행하여 불확실성을 대폭 축소한다.

또한 **'(가칭)사전 적정성 검토제'도 올해 중 도입**한다. 이는 사업자 요청 시 비즈니스 환경을 분석하여 「개인정보 보호법」을 준수할 수 있도록 적용방안을 함께 마련하고, 이에 따른 사업자의 이행결과에 대해 **개인정보위가 적정하다고**

2) 기존 규제에도 불구하고 신기술·신산업 시도가 가능하도록 일정 조건(시간, 장소, 규모) 하에서 규제를 면제·유예해주는 제도

판단한 사안에 대해서는 **행정처분을 하지 않는 제도**이다. 특히 사업자가 신청서를 제출한 시점부터 적용방안 통보까지 **원칙적으로 60일 이내**에 이루어지도록 하여 민간에서 느끼는 법적 리스크를 신속하고 확실하게 줄여나간다.

※ [붙임1] AI 프라이버시팀의 사안별·유형별 지원 방식

2. AI 개발 · 서비스 단계별 개인정보 처리기준 구체화

둘째, **AI 개발·서비스 단계별 개인정보 처리기준과 보호조치, 고려사항** 등을 제시한다. 그간 AI 개발·서비스를 위해 데이터를 수집·이용할 때 개인정보를 어떻게 처리해야 하는지에 대해 별도의 기준이 없었다. 이번 정책방향에서는 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 구체화하였다.

※ [붙임2] AI 개발·서비스 단계별 개인정보 처리원칙(요약)

① 기획 단계 : 개인정보 보호 중심 설계 원칙[3] 반영 → 사전 위험 최소화

AI 모델·서비스를 기획하는 단계에서 **개인정보 보호 중심 설계 원칙**(Privacy by Design)을 반영하여 모델링·학습·운영 과정에서 개인정보 침해 위험을 최소화할 수 있는 방안 등을 안내한다. 또한 이러한 리스크를 파악하고 대응조치를 설계-적용-관리하는 개발자와 개인정보 보호 담당자가 협업하는 **거버넌스 체계를 구축**할 것을 권장하였다.

② 데이터 수집 단계 : 유형별 처리원칙 및 보호조치 준수

데이터를 수집할 때 개인정보의 처리 원칙을 **일반 개인정보, 공개된 정보, 영상정보, 생체인식정보**로 나누어 제시한다. 특히, 대규모 언어모델을 개발하는 경우 **'공개된 정보'**를 부분적으로라도 이용해야 하는 상황이 발생할 수 있는데, 공개된 정보의 처리가 가능한 경우를 체계화하고 이 때 고려해야 하는 사항을 안내하였다. 이와 더불어 「개인정보 보호법」 개정으로 9월 15일부터 시행 예정인 **이동형 영상기기** 규정과 관련하여, 드론·자율주행차 등을 통한 영상의 촬영, 원격관제, 저장, AI 학습 등이 가능한 경우도 안내하였다.

3) 서비스 기획 단계부터 개인정보 처리의 전체 생애주기에 걸쳐 이용자의 프라이버시를 고려한 기술·정책을 설계에 반영하는 것을 의미

③ AI 학습 단계 : 가명처리 특례 및 개인정보 보호 강화 기술 활용

AI 학습 단계에서는 개인정보를 **가명처리**하여 별도의 동의 없이 AI 연구개발이 가능함을 명확히 하였다. 다만, 이 경우에도 다른 정보와의 연계·결합을 통한 재식별 등 **사전·사후적**으로 **발생 가능한 위험**에 대한 **방지조치**가 중요하다는 점을 강조했다. 한편, AI 활용 맥락에서 나타나는 다양한 위험을 사전에 완벽히 제거하는 것은 어려우므로, 이를 **최소화하기 위한 노력 정도**에 따라 **예방조치의 이행 수준**을 판단할 것임을 밝혔다. 또한 합성데이터[4](synthetic data) 등 **개인정보 보호 강화기술**[5](PET ; Privacy Enhancing Technology)을 적극 활용할 것을 권장하였다.

④ AI 서비스 단계 : 투명성 확보 및 정보주체 권리보장 필요

AI 모델을 개발하여 실제 이용자를 대상으로 서비스를 상용화하는 단계에서는 투명성 확보와 **정보주체의 권리보장**이 필요하다는 점을 강조했다. 다만, AI 특성을 고려하여 구체적인 공개범위 및 방법, 권리행사 방안 등에 대해서는 충분한 검토 이후 **가이드라인을 마련**할 것임을 밝혔다. 뿐만 아니라, 기존 AI 모델의 **API를 활용**하거나 기존 서비스에 **플러그인을 추가**하는 경우에도 사용자 등이 개인정보 보호조치를 준수할 수 있도록 상세한 사용지침, 기술문서 등을 제공하는 등 적극적으로 안내해야 한다는 점을 강조하였다.

3. 민 · 관 협력을 통한 분야별 가이드라인 마련

이번에 발표한 정책방향은 **현 시점에서의 기초적인 기준과 원칙**이다. 이를 바탕으로 실제 현장에서 적용 가능하도록 **민간과 협력**하여 세부 분야별로 구체화해 나갈 계획이다. 특히, AI 기업·개발자, 학계·법조계, 시민단체 등 민·관이 함께 논의할 수 있는 **'AI 프라이버시 민·관 정책협의회'**를 오는 10월 중 구성하고, 추진계획에 따라 분야별 AI 환경에서의 데이터 처리기준 등을 공동으로 작업하여 발표할 예정이다.

4) 원본 데이터와 통계적 특성이 유사하여 실제 원본 데이터 분석 결과와 유사한 결과를 얻을 수 있도록 가상으로 재현한 데이터
5) 가명·익명처리 기술, 동형암호, 합성데이터, 차분 프라이버시, 연합학습, 다자간 연산 등 다양한 프라이버시 향상 기술을 통칭

[주요 과제 추진계획(안)]

구분	내용	시기
• 비정형데이터 가명처리 기준	이미지·영상, 음성 등 비정형데이터의 가명처리 기법·사례, 식별위험성 점검기준 등	'23.12월
• 생체인식정보 규율체계	실시간 원격 얼굴인식 기술 제한기준, 영향평가 의무 대상 생체정보 기준 등	'23.12월(법안 마련), ~'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 권리행사 방법 등	'24.6월
• 합성데이터 활용 가이드라인	AI 활용을 위한 합성데이터 생성·처리기준	'24.9월

또한 **PET가 활성화**될 수 있도록 R&D를 확대하고 관련된 가이드라인 등을 마련하는 한편, PET 적용이 모호하거나 검증이 필요한 경우에는 보안성·안전성이 확보된 '**개인정보 안심구역**[6]'에서 기술개발·실증이 가능하도록 할 계획이다.

뿐만 아니라, AI의 리스크 수준에 따라 차등적인 규제 설계가 가능할 수 있도록 위험성에 대해 구체적으로 판단할 수 있는 '**AI 리스크 평가모델**'도 마련한다. 이러한 위험성 평가체계를 구축하기 위해서는 여러 실험과 시도가 필요한 만큼 '**규제 샌드박스'를 활용**하여 AI 분야의 다양한 사례를 축적하고, 이를 바탕으로 운영현황, 위험요인 등을 분석하여 리스크를 식별·평가할 수 있는 체계를 2025년까지 지속적으로 구축해 나갈 계획이다.

4. 국제적 공조체계 강화

마지막으로, AI에 관한 디지털 국제규범 형성을 위해 **글로벌 협력체계**를 공고히 한다. AI는 개발부터 서비스 제공까지 **초국가적인 형태**로 이루어지는 경우가 많아 개별 국가의 규제만으로는 한계가 있고 국제적으로 공조체계가 필수적이다.

6) 데이터 처리의 환경적 안전성을 높여 개인·가명정보를 보다 유연하게 활용할 수 있는 구역('23.10월 시범운영 예정)

개인정보위는 새로운 차원의 디지털 질서 수립을 선언한 **‘파리 이니셔티브’('23.6월)에 입각**하여 AI 개인정보 분야 **국제규범 마련**을 위한 협력체계를 강화해 나갈 계획이다.

지난 6월 서울에서 개최한 「AI와 데이터 프라이버시 국제 컨퍼런스」를 시작으로 **주요국 개인정보 감독기구**와 함께 각 국의 법·정책, 처분 사례 등을 공유하고, AI로 인한 개인정보 침해 이슈 발생 시 신속하게 대응할 수 있도록 한다.

또한 **2025년 글로벌 프라이버시 총회(GPA*)를 유치**하여 AI를 중심으로 디지털 심화 시대에 새롭게 대두되는 프라이버시 이슈에 대해 논의할 예정이다. 그 외에도 여러 논의의 장에 적극적으로 참여하여 새로운 국제 규범 체계의 확립 과정에 주도적 역할을 할 계획이다. 한편, 오픈AI, 구글, 메타 등 **글로벌 AI 사업자**와 **국내 AI 사업자**와의 소통도 활성화한다.

* Global Privacy Assembly, 개인정보 분야 최대 규모의 국제 협의체

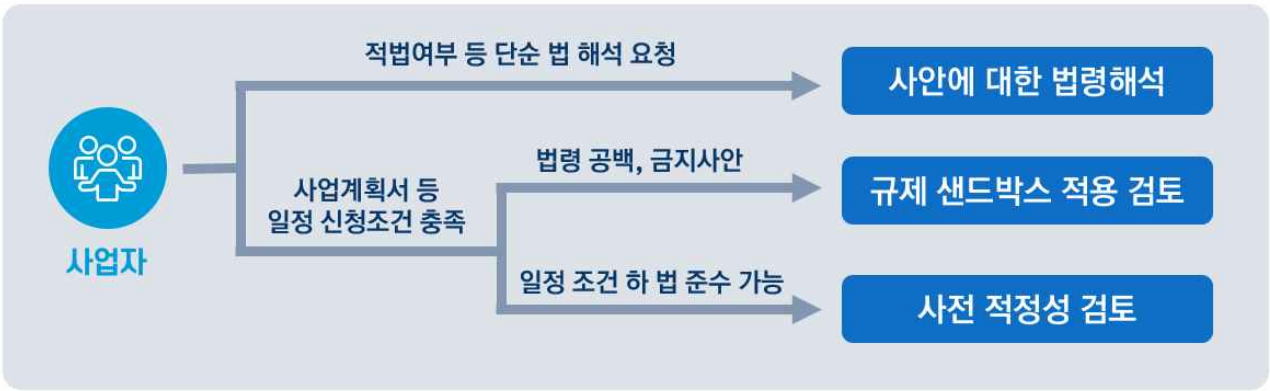
개인정보보호위원회 고학수 위원장은 “이제 AI는 전 세계, 모든 산업에서 기반 기술로서 역할을 하고 있는 만큼 데이터를 어떻게 안전하게 활용할 수 있을지에 대한 새로운 디지털 질서 정립이 필요한 시점”이라면서,

“인공지능에 있어 무조건적인 ‘제로 리스크(zero risk)’를 추구하기 보다는 프라이버시 침해 최소화를 위한 실천적 노력을 경주하는 것이 더욱 중요하다는 인식 하에, 글로벌 규범을 선도할 수 있는 AI 개인정보 규율체계를 확립해 나가겠다.”라고 밝혔다.

담당 부서 <총괄>	개인정보정책국 개인정보보호정책과	책임자	과 장	김직동 (02-2100-3051)
		담당자	서기관	조한아 (02-2100-3052)
			사무관	정영수 (02-2100-3060)
<영상정보, 생체인식정보>	개인정보정책국 신기술개인정보과	담당자	사무관	정종일 (02-2100-3066)
			사무관	이웅비 (02-2100-3065)
<가명정보>	개인정보정책국 데이터안전정책과	책임자	과 장	태현수 (02-2100-3071)
		담당자	사무관	주문호 (02-2100-3088)
<사전 적정성 검토제>	조사조정국 조사총괄과	책임자	과 장	박영수 (02-2100-3101)
		담당자	사무관	장수용 (02-2100-3103)

붙임1 **AI 프라이버시팀의 사안별·유형별 지원방식**

□ 지원방식



❶ 적법여부 등 단순 **법 해석 요청** → 사안별 법령 해석 지원

❷ 기존 **법령에 공백**이 있거나 **현행 규정상 금지**되는 사안
→ 규제 샌드박스(실증특례)를 활용할 수 있는 방안 안내

❸ 일정한 안전조치의 이행 등을 전제로 「**개인정보 보호법**」 **준수**가 가능한 경우 → 사전 적정성 검토제* 적용

- **(개념)** AI 사업자가 모델·서비스 개발 시 **개인정보 보호법을 준수**할 수 있도록 하는 방안을 **개인정보위와 사업자**가 **함께 마련**하고,
  - 위원회가 요구하는 안전조치 등을 충분히 이행하여 적정하다고 판단한 사안에 대해서는 향후 **환경·사정 변화가 없는 한 행정처분을 하지 않는** 제도
- **(신청)** 처리하고자 하는 데이터의 수집방법과 범위, 데이터 처리절차, 예상되는 리스크와 보호조치 계획 등의 내용을 포함한 **사업계획서 등을 첨부**하여 **AI 프라이버시팀에 신청**
  ※ 향후 사전 적정성 검토제의 신청요건 및 구비서류, 절차 등 구체화 예정
- **(기대효과)** 사업 초기 단계부터 법 준수를 위한 방안을 함께 설계·이행함으로써 **개인정보는 충분히 보호**하면서도 **사업을 안정적으로 추진**할 수 있도록 지원

□ 향후계획

○ ‘AI 프라이버시팀’ 신설 및 법령 해석 지원 개시('23.10월중)

○ ‘사전 적정성 검토제’ 도입을 위한 제도개선 및 시범운영('23.하반기 중)

붙임2 AI 개발 · 서비스 단계별 개인정보 처리기준(요약)

단계	처리기준
기획·설계	• **개인정보 보호 중심 설계**(Privacy by Design) 원칙 반영 • AI 단계별 위험 분석 및 대응계획 수립 ※ 위험 등을 파악하고 대응조치를 설계·적용·관리하는 거버넌스 체계 구축 필요
데이터 수집 – 일반 개인정보	• 적법하게 수집한 정보*는 '**수집 목적 범위 내**'에서 이용 가능 * 계약 체결·이행, 법령 준수, 정보주체 동의 등 • 당초 수집 목적과 **합리적으로 관련된 범위**에서 정보주체 이익을 부당하게 침해하지 않는 경우 **추가적 이용 가능**
데이터 수집 – 공개된 정보	• 이익형량 후 ①동의의사가 있다고 **객관적으로 추단**되거나, ②처리자의 **정당한 이익**이 명백히 우선하는 경우 수집·이용 가능 * 저작권법, 부정경쟁방지법, 정보통신망법 등에 따른 사항은 해당 법률을 따라야 함 • 공개된 정보를 크롤링 등으로 수집, **가명처리 후 AI 학습**에 이용 가능
데이터 수집 – 영상 정보	• **(고정형) 당초 설치·운영 목적** 관련 **AI 개발** 가능, 관련 없는 경우 익명·가명처리 필요 - 얼굴인식 등 개인의 특징점을 추출하는 AI 개발은 사전 동의 또는 법령상 근거 필요 • **(이동형)** 당초 촬영목적 달성을 위해 필요한 범위 내에서 **안전 조치 후**에 **원격 관제**, **최소한의 저장** 가능 - **불특정 다수 영상**은 **익명·가명처리**가 필요하나, **샌드박스** 등을 통해 강화된 안전조치* 하 **원본 활용 검토** * 인적 개입 차단, 지속·주기적 점검 등 관리체계 마련, 책임성 강화 등
데이터 수집 – 생체인식 정보	• **별도 동의**가 있거나 **법령 근거**가 있는 경우에만 처리 가능 - 크롤링 등을 통해 공개된 정보에서 생체인식 정보를 추출하여 수집하거나 생성·처리하는 것은 엄격히 제한 • 대체수단 마련, 원본정보 분리 보관 등 **보호조치 이행**
AI 학습	• 과학적 연구 등의 목적으로 **가명처리**하여 동의 없이 **AI 개발 가능** - 다른 정보와의 결합 등을 통한 식별 위험 등을 고려하여 **사전·사후적 예방조치** 필요 * 리스크를 최소화하기 위한 노력 정도에 따라 예방조치의 이행 수준 판단 • 활용목적·처리환경에 맞는 **개인정보 보호 강화기술**(PET) 활용 - **합성데이터, 개인정보 안심구역** 등을 통해 PET 활용기반 조성
서비스 제공	• **AI 학습데이터 수집**방법, 서비스 과정에서 생성되는 정보의 **처리방법** 등 **안내** • 삭제·처리정지·자동화된 결정 대응권 등 **정보주체 권리행사** 보장