개인정보보호위원회 | 보도자료 | 대체불가 대한민국

보도시점 2026.7.23(목) 10:00 배포 2026.7.22.(수) 14:00

국민이 신뢰할 수 있는 공공 인공지능 전환(AX), 프라이버시 보호로 적극 뒷받침

- 개인정보위, 「공공 AX 프라이버시 보호 안내서」 공개
- 실무자가 필요한 핵심 점검사항을 실제 사례와 함께 알기 쉽게 제시

공공부문의 인공지능 전환(AX ; AI Transformation, 이하 'AX')이 본격 추진되는 가운데, 프라이버시를 고려하여 안전하고 신뢰할 수 있는 공공 AX가 추진될 수 있도록 지원하는 안내서가 마련됐다.

개인정보보호위원회(위원장 송경희, 이하 '개인정보위')는 7. 23.(목) 개최된 제11회 과학기술관계장관회의에서 「공공 AX 프라이버시 보호 안내서」(이하 '안내서')를 공개했다

이번 안내서는 공공기관이 AX를 추진하는 과정에서 개인정보 처리 이슈를 미리 확인하고 대응할 수 있도록 돕기 위해 마련됐다.

공공기관은 국민의 일상과 밀접한 행정서비스를 제공하며 복지, 보건, 안전, 민원 등 다양한 분야의 방대한 데이터를 처리한다. 이에 따라 공공 AX의 안전성은 정부 정책과 행정서비스에 대한 국민 신뢰와 직결된다.

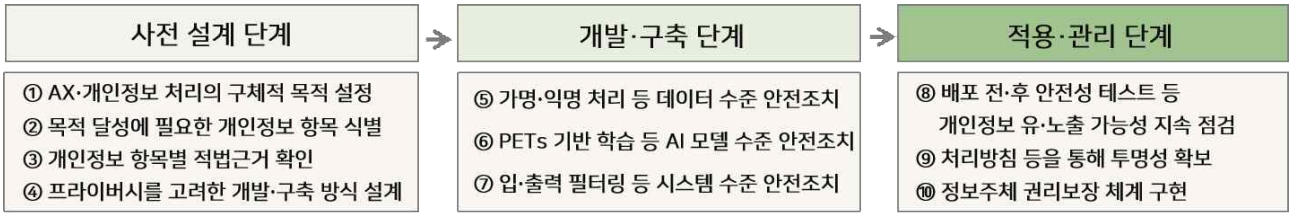
다만 일선 공공기관에서는 개인정보보호와 인공지능(AI) 분야 전문인력이 충분하지 않아 복잡한 AI 데이터 처리방식을 이해하고 구체적인 보호조치를 설계하는 데 어려움을 겪는 경우가 있다. 개인정보위는 이러한 현장의 어려움을 줄이고 공공 AX가 보다 적극적으로 추진될 수 있도록 AI 관련 사전실태점검, 사전적정성 검토 결과 등 실제 사례를 바탕으로 법적기준, 안전조치 등을 안내서에 체계적으로 담았다.

안내서의 주요 내용은 다음과 같다.

첫째, 공공 AX 추진 과정을 세 단계로 나누어 실무자가 확인할 “10대 핵심 점검사항”을 제시했다.

공공 AX 추진 과정을 ▲사전 설계 → ▲개발·구축 → ▲시스템 적용·관리의 세 단계로 구분하고 10대 핵심 점검사항을 제시했다.

< 공공 AX 프라이버시 10대 핵심 점검 >



‘사전 설계’ 단계에서는 AX를 통해 달성하려는 목적과 처리 대상을 명확히 하여 목적제한, 최소수집 등 보호원칙이 준수될 수 있는 기반을 마련하도록 했다. 또한, 처리되는 개인정보 항목별 수집·이용·제공의 적법 근거를 확인하도록 했다. 개발·구축 방식을 선택할 때는 시스템의 성능뿐 아니라 처리되는 개인정보의 성격과 예상되는 프라이버시 위험을 함께 고려하여 적절한 방식을 선택하도록 안내했다.

‘개발·구축’ 단계에서는 학습데이터 활용, 지시어 입력, 검색 증강 생성 연계, 결과 출력 등 개인정보가 처리되는 지점별 안전조치를 적용하도록 했다. 실무에서 검토할 수 있는 안전조치의 내용으로는 학습데이터 가명·익명처리, 차분 프라이버시 등 개인정보보호 강화기술 적용, 개인정보 입력·출력 필터링, 접근권한 관리 등을 제시했다.

‘시스템 적용·관리’ 단계에서는 배포 전·후 테스트 등을 통해 개인정보 유·노출 가능성을 지속 확인하고, 모니터링 및 사고 대응체계를 마련하도록 했다. 또한, 개인정보 열람, 정정·삭제, 처리정지 등 보호법에서 보장하고 있는 정보주체 권리에 대한 보장절차를 수립하도록 하고, 처리방침 등을 통해 개인정보 처리 관련 사항을 투명하게 알리도록 안내했다.

둘째, 공공 AX의 활용 방식과 위험 수준에 따라 필요한 보호조치를 차등화하여 제시했다.

공공 AX를 ▲기초업무 보조, ▲정보 연계·분석·추천, ▲선별·판단의 세 가지 유형으로 구분하고, 모든 AI 시스템에 동일한 조치를 일률적으로 요구하기보다는 구체적 맥락에 따라 필요한 사항을 유연하게 검토할 수 있도록 했다.

< 공공 AX 프라이버시 유형별 점검 >

기초 업무 보조	정보 연계·분석·추천	선별·판단
안전한 활용 환경 조성, 기본적 안전조치에 중점	목적 외 이용 및 개인정보 추론 리스크 집중 관리	엄격한 적법성 검토, 자동화된 결정에 따른 리스크 관리
① 이용지침 안내 등 안전한 이용환경 조성 ② 오남용, 외부공격에 대한 시스템 안전성 확보 ③ AI 입·출력 데이터의 적절한 관리	④ 외부 DB·시스템 연계 시 적법근거 검토 ⑤ 추론 수준 및 입력데이터 최소화·추상화 ⑥ 복잡한 데이터처리의 가시성, 통제가능성 확보	⑦ 보다 엄격한 적법성·비례성 검토 ⑧ 부정확한 처리 등에 따른 권리침해 방지 ⑨ 자동화된 결정에 따른 권리침해 방지

대규모 언어모델을 활용한 자료 가공·요약·검색, 챗봇 상담 등 '기초업무 보조' 유형은 안전한 이용환경 조성과 기본적인 안전조치를 중심으로 안내했다. 허용·금지되는 활용 사례를 명확히 하여 주요 사용자를 대상으로 안내 및 교육하고, AI 입력·출력 데이터 등에 대한 관리체계를 수립하도록 안내했다.

여러 데이터베이스와 시스템을 연결해 맞춤형 정보를 분석하거나 추천하는 '정보 연계·분석·추천' 유형은 목적 외 이용과 과도한 개인정보 추론 위험을 중점적으로 살피도록 했다. 외부 데이터베이스(DB)를 연계할 때 처리 근거 미비가 없도록 확인하고, 분석·추론되는 정보도 목적 달성에 필요한 수준으로 제한하여 사생활 침해를 최소화하도록 했다. 또한 연계된 데이터베이스(DB) 및 시스템에 대하여 접근권한을 차등 부여, 접근통제하는 등 강화된 관리체계를 구현하도록 안내했다.

행정 수혜자 선별, 위험 탐지 등 공공 의사결정에 직접 활용되는 '선별·판단' 유형은 AX 및 개인정보 처리의 필요성·효과성, 법적 근거를 보다 면밀하게 검토하도록 했다. AI의 편향과 정확성·강건성 부족으로 인해 정보주체 권리침해가 발생하지 않도록 관련 데이터의 정확성·대표성, 시스템의 성능을 지속 점검·개선할 수 있도록 했다. 또한, 자동화된 결정에 해당하는 경우 보호법에서 보장하는 거부권, 설명·검토 요구권 등 정보주체의 권리가 실질적으로 보장될 수 있도록 대응체계를 마련하도록 안내했다.

셋째, 안전한 AX를 위한 각 공공기관의 역할과 개인정보위의 역할을 제시했다.

각 공공기관은 기관장, 개인정보 보호책임자(CPO), 최고인공지능책임자(CAIO) 등을 중심으로 개인정보 보호를 공공 AX의 핵심 요소로 인지하고, 개인정보보호 부서, AX 현업부서 등 관련 부서 간 협력체계를 구축하는 것이 바람직하다. 또한, AI 운영환경을 고려하여 내부 관리계획을 고도화할 필요가 있다.

개인정보위는 공공기관의 애로사항 해소를 밀착 지원하기 위해 '공공 AX 프라이버시 헬프데스크'를 상시 운영한다. 헬프데스크는 공공기관의 문의 내용과 사업 특성에 따라 ▲법령 해석, ▲사전적정성 검토제, ▲가명정보 처리 지원, ▲규제 샌드박스 등 적합한 지원제도와 연계하는 종합창구다.

※ 공공 AX 프라이버시 헬프데스크 안내 : 02-2100-3072, 3169

송경희 개인정보위 위원장은 "공공 AX는 국민에게 더 빠르고 편리한 서비스를 제공하고, 공무원이 보다 효율적으로 일할 수 있도록 하는 정부 혁신의 핵심 수단"이라며, "개인정보위는 공공기관이 프라이버시에 대한 불확실성 때문에 혁신을 주저하지 않도록 구체적인 기준과 실무적인 해결방안을 제공하고, 공공 AX가 안전하고 신뢰할 수 있는 방식으로 확산될 수 있도록 적극 지원하겠다."라고 말했다.

담당 부서	개인정보정책국 인공지능프라이버시팀	책임자	팀장(代) 임수연 (02-2100-3078)

붙 임 공공 AX 프라이버시 보호 안내서 개요

□ 개요

○ 공공 AX 추진 시 **개인정보보호**와 관련한 **어려움을 해소**하기 위한 **실무 지침**으로서, **안전하고 적법**한 공공 AX를 위한 **핵심 점검사항** 안내

□ 주요 내용

○ **(10대 핵심점검)** 사전 설계, 개발·구축 단계, 적용·관리 단계별 **보호 원칙 준수, 적법근거 식별, 안전조치 적용** 등 핵심점검 사항 제시

사전 설계 단계	개발·구축 단계	적용·관리 단계
① AX·개인정보 처리의 구체적 목적 설정 ② 목적 달성에 필요한 개인정보 항목 식별 ③ 개인정보 항목별 적법근거 확인 ④ 프라이버시를 고려한 개발·구축 방식 설계	⑤ 가명·익명 처리 등 데이터 수준 안전조치 ⑥ PETs 기반 학습 등 AI 모델 수준 안전조치 ⑦ 입·출력 필터링 등 시스템 수준 안전조치	⑧ 배포 전·후 안전성 테스트 등 개인정보 유·노출 가능성 지속 점검 ⑨ 처리방침 등을 통해 투명성 확보 ⑩ 정보주체 권리보장 체계 구현

○ **(유형별 중점검토) 기초업무 보조, 정보 연계·분석·추천, 선별·판단** 등 AI의 구체적 **용례별 중점 검토사항** 안내

기초 업무 보조	정보 연계·분석·추천	선별·판단
안전한 활용 환경 조성, 기본적 안전조치에 중점	목적 외 이용 및 개인정보 추론 리스크 집중 관리	엄격한 적법성 검토, 자동화된 결정에 따른 리스크 관리
① 이용지침 안내 등 안전한 이용환경 조성 ② 오남용, 외부공격에 대한 시스템 안전성 확보 ③ AI 입·출력 데이터의 적절한 관리	④ 외부 DB·시스템 연계 시 적법근거 검토 ⑤ 추론 수준 및 입력데이터 최소화·추상화 ⑥ 복잡한 데이터처리의 가시성, 통제가능성 확보	⑦ 보다 엄격한 적법성·비례성 검토 ⑧ 부정확한 처리 등에 따른 권리침해 방지 ⑨ 자동화된 결정에 따른 권리침해 방지

○ **(실행체계)** 각 기관은 **개인정보보호를** 공공 AX에 내재화할 수 있도록 **CPO의 권한·역할, 관련 부서간 협력, 내부관리계획 고도화** 등 추진

- **개인정보위**는 공공AX 프라이버시 **헬프데스크**를 통한 **밀착 지원**, 가이드라인 등 **AI 규범 정립** 등 추진

□ 향후 계획

○ 『공공 AX 프라이버시 헬프데스크』('26.1~)를 통해 맞춤형 상담 지원(계속)