개인정보보호위원회 **보도자료** 대체불가 대한민국

보도시점 2026.7.3.(금) 10:00 배포 2026.7.2.(목) 17:30

신뢰로 여는 인공지능(AI) 혁신, 달라지는 개인정보 체계로 이끈다

- 「신뢰 기반의 인공지능 혁신을 촉진하는 제3차 개인정보 보호 기본계획('27-'29)」 발표
- 위험비례 규율, 예방중심 보호, 범정부 협력, 원스톱 국민 권리구제 체계 확립 등 인공지능 시대 정책적 요구에 적극 대응하는 개인정보 정책 청사진 제시

개인정보보호위원회(위원장 송경희, 이하 "개인정보위")는 7월 3일(금) 열린 경제관계장관회의에서 관계부처 합동 안건으로 「신뢰 기반의 인공지능(AI) 혁신을 촉진하는 제3차 개인정보 보호 기본계획(2027-2029)」(이하 "기본계획")을 발표하였다.

이번 기본계획은 개인정보위가 법에 따라 3년마다 중앙행정기관의 장과 함께 수립하는 계획으로, 인공지능 대전환에 따른 데이터 활용 수요 증대와 반복되는 대규모 개인정보 유출이라는 당면환경에 대응하여 향후 3년간 추진할 개인정보 정책의 청사진을 마련한 것이다.

기본계획은 "신뢰받는 개인정보 환경, 안심하고 누리는 인공지능(AI) 사회"를 비전으로 ▲인공지능 대전환 시대 개인정보 보호체계 혁신, ▲사전예방 중심 보호체계 확립, ▲전략적 개인정보 정책 고도화, ▲국민 권익 증진 및 신뢰문화 정착이라는 4대 전략과 12대 추진과제를 중심으로 마련되었다.

1 인공지능 시대 신뢰기반 데이터 활용을 촉진하기 위해 개인정보 보호체계를 혁신한다.

먼저, 인공지능 환경을 유연하게 반영하는 규율체계로의 전환을 추진한다. 인공지능 환경 이전에 설계된 일률적 규제로 법령 준수가 어렵고 데이터 활용에 제약이 있다는 현장의 목소리를 반영하여, 위험에 비례한 보호를 규율하는 원칙 중심 보호체계로 전환한다.

이와 함께, 인공지능 전환(AX) 과정에 수반되는 개인정보 처리의 불확실성을 신속하게 해소하기 위해 맞춤형 혁신지원 종합 창구로서 '인공지능 전환(AX) 안심지원센터'도 운영할 계획이다. 나아가, 5극3특 균형성장 전략에

발맞춰 전국 어디서나 접근 가능한 데이터 혁신 환경을 조성하기 위해 지역 거점별 데이터(가명·익명) 연계·활용 허브를 구축·확대한다.

그간 기업·기관 중심으로 이뤄진 데이터 활용에 대한 국민주권도 강화한다. 국민이 내 정보에 대한 결정권을 갖도록 마이데이터 지원(온마이데이터) 플랫폼을 강화하고, 데이터로부터 산출된 가치에 대한 정보주체 환원 체계를 수립하고 확산한다. 10대 분야 확대 등 마이데이터 1단계를 완수하고, 마이데이터 2단계 추진을 통해 복지·돌봄·의료 등 데이터 기반 사회적 난제 해결에 앞장선다.

아울러, 인공지능 데이터 신뢰 확보를 위한 프라이버시 리스크 대응을 강화한다. 자율형 인공지능(에이전틱 AI)에 의한 처리 등 의사결정의 책임구조 검토, 실물 인공지능(피지컬 AI)의 상시적 정보 수집 확대에 대응하는 권리보장, 위험평가 등 최신 기술에 대한 규율체계와 보호 기준도 수립한다.

또한, 급변하는 인공지능 사이버 위협에 선제적으로 대응하여 리스크 관리 모델 및 환경변화를 반영한 안전조치 기준도 제시한다. 디지털 환경에서 개인 권리 보호를 위한 개인정보 정확성 및 투명성 확보가 강조되면서, 딥페이크(deepfake) 등 데이터 변조 방지 방안 마련, 인공지능 투명성 확보 제도화도 추진한다.

2 둘째, 개인정보 보호체계를 사전예방 중심으로 정착시킨다.

먼저, 유출사고가 발생한 후에는 온전한 피해 회복이 어렵다는 점을 고려하여 사전예방 중심의 보호체계를 확립하고 현장 정착 및 내재화를 지원한다.

고위험군 집중점검, 부처 합동점검 등 상시적 점검 체계를 고도화하여 사고 발생 전 취약점이나 보호 조치를 미리 점검하여 개선하는 데 집중한다. 이와 함께, 취약점 점검 등 범정부적 상시적 방어체계를 확립하고 인공지능 보안 점검 등 보안점검 제도화를 추진해나간다.

정보보호 및 개인정보보호 관리 체계(ISMS-P) 인증 및 각종 평가체계에 인공지능 기술을 접목하여 기준과 절차를 개선하여 실효성을 높인다. 특히, 국민의 개인정보를 다량 보유·처리하는 공공분야는 안전조치 기준 강화, 상시적 점검체계 확대, 평가제도의 실효성 제고를 우선 추진하여 보호 수준을 획기적으로 개선한다.

다음으로, 사고 전 선제적 보호조치에 대한 강력한 유인체계를 강화하고 기업의 책임성을 강화한다. 의무기준을 넘어서는 선제적인 보호 투자 시에는 유출 과징금을 감면하는 등 인센티브 사례를 확산하여 기업의 자발적 보호조치를 적극 유도한다. 나아가, 조직 의사결정 과정에 개인정보 보호가 적극 고려될 수 있도록 대표자(CEO) 책임을 정착하고 개인정보보호책임자(CPO)의 위상도 한층 강화한다.

반면, 관리의무 소홀 등 법 위반에 대해서는 엄정 조사·제재로 억지력을 대폭 강화한다. 이를 뒷받침하기 위해 조사 실효성 확보를 위한 이행강제금 도입 등 제도개선을 추진하고, 기술분석 환경 구축·확대 등 과학적 조사를 위한 역량도 지속 강화한다. 개인정보 불법유통에 대해서는 형사처벌 근거를 신설하고, 탐지·삭제 및 관련 정보 수집·분석 등 정부의 역할을 강화한다.

아울러, 기존 유출 시 조사·제재 중심으로 대응했으나, 상시적 유출 위협 환경을 고려하여 '회복력(resilience) 지원' 중심으로 대응 인프라를 재정비한다. 중소기업 유출 발생 시 복구 기술지원 중심으로 대응하고, 사고 이전에도 중소·영세기업에 맞춤형 컨설팅, 보호·보안 지원 사업을 제공한다. 이를 통해 보호·보안 산업 육성을 지원하고, 산업계 전반의 보호수준을 상향평준화 할 수 있는 기반을 수립해나간다.

사고 대응이 가능한 개인정보 보호 특화 전문인력을 양성하여 회복력 강화를 지원하고, 인력풀의 효과적인 활용을 위해 인공지능 보안인력 관리 플랫폼을 구축한다. 아울러, 암호기술 등 개인정보보호 강화기술(PET) 연구개발(R&D) 지속 확대를 통해 전 분야 보호 인프라를 강화한다.

한발 나아가, 실물 인공지능(피지컬 AI) 환경 확산에 대응하여 디지털 보안과 물리 안전 규제에 대한 사이버-물리 통합보안 체계도 검토하고, 자율형 인공지능(에이전틱 AI) 기반의 공격을 반영한 안전조치 기준 개선을 추진한다. 상시적 방어체계 강화를 위해 취약점 발굴·대응 등 관련 산학연·범부처 협력도 강화한다는 계획이다.

3 셋째, 범정부 보호 협력체계 및 안전한 국경간 데이터 이전 체계를 고도화한다.

전 산업 분야에서 개인정보 활용 확대를 고려하여, 개인정보 보호가 범정부

차원의 과제로 이행되도록 범부처 협력체계를 확립한다. 통신, 교육, 고용 등 상대적으로 위험성이 높은 분야는 개인정보위와 소관부처가 공동 점검·관리하는 체계를 수립하고, 개인정보 위협 요소에 대한 조기경보체계를 구축하여 위기대응 역량 강화를 추진한다.

아울러, 디지털 환경의 규제 체계 간 정합성도 확보한다. 개인정보 중복 규제 등을 합리적으로 조정하여 체계를 정비하고, 금융·공정거래 등 관련 규제기관 간 협력을 강화한다. 인공지능 및 데이터 정책 소관 기관과도 긴밀하게 협력하여 디지털 분야의 법령 간 적용 관계를 명확화한다.

생성형 인공지능, 클라우드 환경 등 국외이전 수요가 증가함에 따라 데이터 이전 네트워크도 확대한다. 이미 수립된 한-EU 상호 동등성 인정 체계에 이어, 영국, 일본, 미국 등 법체계 유사성, 교역규모 등을 고려한 맞춤형 대응으로 데이터 상호 이전 네트워크를 확대해나간다. 이와 함께, 보호수준이 상대적으로 미흡한 국가로의 데이터 관리 대응력 강화로 안보위협을 최소화한다.

국외이전 확대에 대응하여 제도적 기반도 지속 개선해나간다. 안전한 국외이전 수단(SCC*, BCR**)을 확대하여 글로벌 공동 연구 등 국경간 데이터 이전에 대한 유연성을 확보한다. 이와 동시에, 국외이전 현황조사를 실시하고, 국외이전 영향평가를 신설하는 등 리스크 관리체계 수립을 병행한다.

* SCC(Standard Contract Clauses, 표준계약조항) 개인정보를 이전하고 받는 경우 준수해야 할 계약상 의무를 통해 국외로 이전된 후에도 보호 수준 유지

** BCR(Binding Corporate Rules, 구속력있는 기업규칙) 다국적 기업 내에서 발생하는 개인정보의 국경 간 이전을 위해 기업에서 정하여 감독기관의 승인을 받아 이행하는 법적 구속력이 있는 기업내 개인정보 보호 규정

4 넷째, 국민 권익을 증진하고 일상 속 프라이버시 보호를 강화하여 신뢰를 확립한다.

최근 유출 피해를 경험한 국민이 늘어나면서 간편한 권리구제 방안에 대한 요구가 증대됨에 따라, 유출·침해 시 신고부터 조사, 분쟁조정, 손해배상까지 모든 절차를 연계하는 원스톱 권리구제 체계를 마련한다. 또한, 인공지능 기반으로 개인정보 관리 플랫폼을 구축하여 국민이 쉽게 자신의 개인정보 처리 현황을 확인하고 권리를 행사할 수 있도록 지원한다.

이와 함께, 정보주체 권리보장을 강화하기 위한 제도 기반도 수립한다. 정보주체 권익 증진 전문기관 수립 및 피해회복 동의의결제 추진, 적극적 분쟁조정 등을 통해 신속한 피해보상 및 분쟁해결 제도 실질화를 추진한다.

나아가, 일상 접점에서 발생하는 프라이버시 침해 우려도 적극 해소한다. 특히, 디지털 환경에서 영상·생체정보 등 상대적으로 민감도가 높은 정보의 수집·이용이 보편화됨에 따라 특화된 보호가 가능하도록 규율체계를 개선하고, 아동·청소년 등 권리행사 취약계층에 대해서도 보호 체계도 강화한다.

이번 기본계획은 인공지능 사회 도래에 대응하는 개인정보 보호체계를 확립하고, 국민 신뢰를 바탕으로 데이터가 안전하게 활용되는 인공지능 혁신 환경을 조성하는 데 중점을 두었다. 이를 바탕으로 부처별 시행계획을 수립하고 이행함으로써 국민이 안심하고 향유할 수 있는 인공지능 사회 도래를 지원해 나갈 예정이다.

송경희 개인정보보호위원장은 "이번 3개년 기본계획은 개인정보 규율체계를 인공지능 환경에 맞게 재설계하고 사전 예방 중심의 보호체계를 확립함으로써, 국민은 안심하고 인공지능 편익을 누리고 기업은 신뢰를 바탕으로 혁신하는 환경을 만들어 나가는 데 정책 역량을 집중하겠다"라고 밝혔다.

담당 부서	개인정보 보호정책과	책임자	과 장	최윤정	(02-2100-3051)
		담당자	사무관	이정수	(02-2100-3052)
			사무관	고채린	(02-2100-3056)

붙임1 「제3차 개인정보 보호 기본계획 (2027-2029)」 비전 및 전략

붙임2 「제3차 개인정보 보호 기본계획 (2027-2029)」 주요 내용

신뢰 기반의 AI 혁신을 촉진하는 제3차 개인정보 보호 기본계획

1 수립 배경

□ AI 대전환 등 **사회 변혁**에 따라 **데이터 활용 수요**가 폭증하면서, 이에 부응하는 **개인정보 제도 혁신** 및 적극적 혁신지원 **필요 증대**

○ **유럽, 일본 등 세계 각국**에서도 **AI 시대**의 안전한 개인정보 **활용**을 촉진하기 위한 **개인정보 및 AI 분야 제도개선 적극 추진 중**

□ 한편, **통신·유통** 등 **민간 분야**뿐 아니라 **공공분야**까지 파급력 높은 **개인정보 유출 사고**가 **연이어 발생**, 유출 **빈도·규모**가 **지속 증가***

* **(유출신고)** '20년219건 →'25년447건(2배↑), **(유출규모)** '20년12,003천건 → '25년103,546천건(8.6배↑)

○ 향후 **AI 기반 공격기술** 고도화로 **사이버 위협 증가가 예견**되면서, **전 분야**에 **상시적 방어·관리** 체계로의 **근본적 전환 시급**

□ 아울러, **개인정보**의 중요성에 대한 **국민 인식**이 높아져 **투명성 보장** 및 **유출 시 손해배상** 등 **적극적 권리행사 방법**에 대한 **요구 확대**

⇒ **신뢰 확보를 위한 보호체계 강화 및 데이터 기반 혁신을 뒷받침하는 개인정보 제도 설계를 통해, 국민이 안심하고 향유하는 AI 시대 촉진**

2 현황 및 문제점

1 **(데이터 활용)** AX **데이터 수요** 폭증 및 **데이터 활용방식 변화**로 인해 **법적 불확실성이** 증가하고 예측하기 어려운 **프라이버시 이슈 확대**

2 **(사고예방)** 기존의 관리·점검 체계가 **사후제재 중심으로 설계**되어 **기업· 기관**의 **사전 예방 역량** 및 유출 사고 시 **회복력 미비**

3 **(거버넌스)** **디지털 규제 환경** 복잡화로 **범정부 협력체계 정비 필요**, **데이터 국외 이전 원활화** 및 불법유통 등 **공동대응 이슈 발생**

4 **(국민체감)** 침해신고, 손해배상 등 **권리구제 제도의 접근성 제약**, 일상 속 **영상·생체정보** 이용 증가 등 **취약분야·계층 보호 필요** 증대

3 추진전략 및 과제

비 전 신뢰받는 개인정보 환경, 안심하고 누리는 AI 사회

추진 전략

1. AI 대전환 시대 개인정보 보호체계 혁신
2. 사전예방 중심 보호체계 확립
3. 전략적 개인정보 거버넌스 고도화
4. 국민 권익 증진 및 신뢰문화 정착

1. AI 대전환 시대 개인정보 보호체계 혁신 개인정보위 · 복지 · 과기

AS-IS (2026)		TO-BE (~2029)
▪ 과거 일률적 규제가 AI 환경과 충돌하고 불확실성이 증대되어 데이터 활용 제약	→	▪ 위험도에 비례한 유연한 규제체계, 맞춤형 지원 강화로 데이터 혁신 촉진

□ AI 환경을 유연하게 반영하는 개인정보 규율체계로 전환

○ 원칙중심 규제로 **데이터 처리 유연성 확보** 및 **안전활용 적극 지원**

- AI 확산 전에 설계된 **일률적 규제** 대신 **위험 비례 규율체계**로 **전환**
- **맞춤형 혁신지원 종합 창구**(가칭 AX 안심지원센터)를 본격 운영하고, **전국**에서 **데이터**(가명·익명) **연계·활용**이 가능한 **지역 거점별 허브 구축**

※ 안전조치 전제로 **AI 학습에 불가피**한 **개인정보 원본 활용을 허용**하는 **AI 특례 도입 병행**

○ 개인이 **내 정보 활용**에 대해 **스스로 결정**하게 하고(온마이데이터 플랫폼), **산출된 가치**를 **정보주체에게** 돌려주는 **가치환원 체계 수립·확산**

- **2단계 마이데이터** 추진('27년~)을 통해 **데이터 융합기술** 기반으로 **복지·돌봄·의료** 등 **사회적 난제해결** 추진

□ AI 기본사회에 대비한 프라이버시 리스크 대응 강화

○ **에이전틱 AI 의사결정 책임구조** 검토, **피지컬 AI**의 **상시적 정보 수집** 환경에 대응한 **권리보장, 사전 위험평가** 등 **신기술 규율체계 설계**

- 급변하는 **AI 사이버 위협**에 **선제 대응**하는 **리스크 관리모델** 고안

○ **정확성·투명성** 확립을 위해 **딥페이크·사칭 방지** 및 **AI 투명성 제도화**

2. 사전예방 중심 보호체계 확립 개인정보위 · 과기 · 국정 · 중기 · 경찰

AS-IS (2026)		TO-BE (~2029)
▪ AI 사이버 위협 현실화에도 불구, **사후대응 중심 관리**로 권리보호에 한계	→	▪ **상시점검** 및 **선제적 보호조치** 유인 강화로 **사전예방 중심 체계 확립**
▪ 유출 사고 시 **조사·제재 중심** 대응으로 **사고은폐 등 부작용 발생**	→	▪ **'회복력 지원' 중심** 대응으로 전환하여, **신속 회복** 및 **역량강화 지원**

□ 상시적 점검·방어 체계를 통한 사고예방 강화

○ 고위험군 집중점검, **부처 합동점검** 등 **상시 점검·개선 체계**를 구축하고, **AI 기술을 접목한 인증·평가** 도입으로 **全분야 사고예방 체계 확립**

- 특히, **공공분야는 추가 안전조치** 기준 강화, 상시점검 및 **평가제도 실효성 개선**을 **우선적으로 추진**하여, **공공 보호수준 획기적 개선**

※ **공공부문** 개인정보 보호에 대한 **인적·물적 투자** 및 **보호역량 확보** 지원 **적극 추진**

○ **취약점 점검·공개** 제도 등 **범정부 상시적 방어체계**를 확립하고, **AI 보안점검 실시**, 상시점검 테스트베드 구축 등 **보안점검 제도화**

□ 사고 前 선제조치를 위한 책임성·유인체계 정착

○ **선제적 보호투자** 시 **유출 과징금을 감면**하는 등 **적극적인 인센티브**를 강화하고, **대표자(CEO) 및 CPO**의 **법적 책임·역할**의 **현장 안착 지원**

○ **조사 역량 강화**(포렌식 고도화, 기술분석 환경 구축), **조사 실효성 강화**(이행강제금)를 통해 **개인정보 감독** 기능 및 **법 위반 억지력 대폭 강화***

* 불법유통 **처벌근거 신설**, 탐지·삭제 고도화 등 **개인정보 불법유통 대응 강화 병행**

□ 회복력(resilience) 강화를 위한 보호 인프라 구축

○ **중소기업 유출시** 복구·대응 **기술지원** 중심으로 전환하여, 사고 은폐 및 유사사고 재발방지를 위한 **회복력**(resilience) **중심 대응체계 확립**

- 아울러, **보호·보안 산업 육성 지원**을 통해 보호 역량 **상향평준화** 견인

○ **피지컬 AI 확산**에 대응하는 **사이버-물리 통합보안 체계** 수립 및 **에이전틱 AI 기반 공격 증가**를 고려한 **안전조치 기준 개선** 추진

○ **암호기술** 개발 및 **개인정보보호 강화기술**(PET) **연구개발**(R&D) **확대**를 추진하고, 보호 **특화 전문인력 양성** 및 **AI 보안인력 플랫폼 구축**

3. 전략적 개인정보 거버넌스 고도화 개인정보위 · 전부처

AS-IS (2026)		TO-BE (~2029)
▪ 개인정보 보호·활용 규율이 **분야별로 별도 운영**되어 **혼선 및 보호수준 상이**	→	▪ 개인정보위를 **컨트롤타워**로 하여 **범정부 통합 보호체계** 확립
▪ AI, 클라우드 이용 등 **국외이전 제약 발생**	→	▪ **국외이전 수단 신설** 및 **네트워크 확대**

□ 범정부 보호 협력체계 확립

○ **통신, 교육, 고용** 등 리스크가 높은 분야는 **소관부처 공동관리 강화**

- 개인정보 위협 발생 시 **조기경보체계** 구축 등 **위기대응 역량 강화**

○ **중복규제 해소**, 디지털 **규제 정합성 확보** 등 **범정부 협력체계 강화**

□ 안전한 데이터 이전 네트워크 확대

○ 동의 외 **국외이전 수단**(SCC, BCR) **신설**로 유연성을 확보하는 동시에, **국외이전 현황조사** 실시 및 **영향평가 신설** 등 **관리체계 확립 병행**

- 英·美·日 등 **데이터 상호 이전 네트워크** 확대 및 **안보위협 최소화**

4. 국민 권익 증진 및 신뢰문화 정착 개인정보위 · 법무

AS-IS (2026)		TO-BE (~2029)
▪ **유출, 침해 증가**로 불안 증대, **간편·통합 권리구제 창구**에 대한 **국민적 요구 증대**	→	▪ **신고, 분쟁해결, 손해배상** 등 **도구 제공** 및 일상 보호 강화로 **통제권·효능감 회복**

□ 원스톱 국민 권리보장 지원체계 완비

○ 유출·침해 발생시 **신고부터 손해배상**까지 **모든 절차를 해결**할 수 있는 **원스톱 지원체계를 구축**하고, **AI 기반 정보주체 권리행사 도구*** **개발**

* 개인정보 처리현황을 쉽게 파악하고, 권리행사를 간편하게 지원하는 **AX 플랫폼 도입**

○ 정보주체 **권익 증진 전문기관** 수립, 피해회복 **동의의결제 도입** 추진, **적극 분쟁조정** 운영 등 **신속한 피해보상 및 분쟁해결 제도 실질화**

□ 일상 속 체감 프라이버시 보호 강화

○ **디지털 환경**에서 **영상 촬영, 생체인증** 등 **취약성**이나 **민감도가 높은 정보 이용**이 **일상화**됨에 따라, **특화된 보호 및 규율체계 수립**

- **아동·청소년 프라이버시** 보호 정책 강화 등 **취약계층 특별 보호**