발간등록번호
11-1790365-100043-13

2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵

개인정보보호위원회
Personal Information Protection Commission

발간등록번호
11-1790365-100043-13

2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵

개인정보보호위원회
Personal Information Protection Commission

2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵

안내 사항

발간 목적

「개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵(2026~2030)」은 AI 확산에 따른 신기술 등장 및 확산, 국제 규범 변화 등에 맞추어 개인정보 분야 정책과 연계한 기술 및 표준화 연구를 선도적으로 추진하기 위한 목적으로 마련되었습니다. 종전의 분리되어 있던 기술 R&D와 표준화 로드맵을 하나로 통합·연계하여 조기 개정하였으며, 관련 연구를 진행하는 산·학·연 등에서는 개인정보 분야의 기술개발 성과가 국제표준으로 이어질 수 있는 선순환 체계를 조성해 나아가는데 활용하여 주시기 바랍니다.

재검토 기한

로드맵의 최신성을 유지하기 위하여 발간일(2026년 6월) 기준으로 5년마다(매 5년이 되는 해의 6월 30일 전까지) 보완 및 신기술 수요 등을 반영하도록 개정여부를 검토할 예정입니다.

저작권 표시

* 출처 : 개인정보보호위원회, 「개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵(2026~2030)」, 2026.06

문의처

로드맵 내용 관련 문의는 개인정보보호위원회 신기술개인정보과(☎02-2100-3068, 3069)로 개인정보보호 법령 질의 등에 관한 사항은 개인정보보호위원회 법령해석 지원센터(☎02-2100-3043)으로 문의주시기 바랍니다.

관계법령

「개인정보 보호법」 제7조의8 등

※ 법령 최신 자료는 국가법령정보센터(www.law.go.kr), 개인정보 보호 안내서 최신 자료는 개인정보보호위원회 누리집*, 개인정보 포털**을 참고

* 개인정보보호위원회 누리집(www.pipc.go.kr) : 정책·법령 〉 기업정책 〉 기업정책 자료실

** 개인정보 포털(www.privacy.go.kr) : 자료 〉 자료보기 〉 정책자료

목 차

2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵

I 추진배경

CHAPTER I

추진배경

인공지능(AI)·데이터 경제가 성장하면서 규율환경이 변화

- '데이터 주권, 사전예방 보호조치, 안전한 인공지능(AI)'이 미래 성장전략의 핵심 축으로 부상

  - 특히, AI·블록체인·마이데이터·데이터스페이스 등 데이터 기반 산업이 빠르게 확대

- 국내 데이터 산업의 성장으로 개인정보 보호에 필요한 법·정책*, 각종 안내서 등 안전한 활용을 가능케 하는 규율체계를 마련

  * 개인정보 보호법 개정, AI 기본법 제정, 전분야 마이데이터 시행 등

- 신기술 정책이 안전성·투명성·책임성을 요구하는 글로벌 추세*임을 반영하여 국제 표준으로 선도하는 기술 연구개발 성과로 이어질 필요

  * 유럽연합(EU) AI Act, 미 국립표준기술국(NIST) AI RMF, 경제개발협력기구(OECD)·G7 원칙 등

PET-AI 융합 및 시장·기술의 성장

- 전 세계 PET 시장은 50억 달러('26년)에서 312억 달러('34년)까지 성장 전망

  ※ Privacy Enhancing Technologies Market Size, 2021-2034 (Fortune Business Insights, '26)

  - 현장은 PET 솔루션·서비스 개발에 중점을 둔 기술 연구 및 투자가 이뤄지고 있으며, 현재 북미지역이 가장 큰 시장 점유율(약 38%) 차지

  ※ 국내: 금융(자금세탁방지·고객신원확인), 의료(병원 간 데이터 결합·AI 진단), 공공·통계(합성데이터·차분 프라이버시 기반 공개) 등에서 실증 사례가 확대되는 추세

- AI 기술이 일상화되는 시대에 국민·기업이 개인정보를 안전하게 활용할 수 있도록 특화된 기술이 연구·개발(R&D)로 이어지는 추세

  - 국내의 개인정보 보호를 위해 최우선적으로 필요한 정부정책으로 기술개발 및 보급 필요성이 공공·민간 부문 모두에서 상위권* 차지

  * '24 개인정보보호 및 활용조사 결과: 공공부문 1위(65.7%), 민간부문(종사자 수 300인 이상 기업) 2위(36.9%)

- 국외(OECD, 英 ICO 등)에서도 개인정보보호 강화 기술(PET)*을 개인정보 보호 규제 준수와 신뢰 기반의 AI 모델 공유를 위한 핵심 요소로 규정

  * 개인정보를 안전하게 수집·처리·분석·공유할 수 있는 기술 관련 절차, 방법, 지식 등을 모두 포괄

  - PET는 개인정보를 공개하지 않은 상태에서 계산·분석을 수행하며, 기술 적용 시에 개인정보 보호와 함께 본래의 활용목적 달성 가능

※ (주요기술) 연합학습, 차분 프라이버시, 동형암호, 안전한 다자간 연산, 합성데이터 등

AI 환경에 대응 가능하도록 기술 R&D 및 표준화 로드맵 개정 필요

- 기존 개인정보 보호·활용 기술 R&D 로드맵('22~'26)은 전통적 법·제도 및 PET 개발 중심으로 구성되어 신산업·정책과 연계 등에 한계

  - AI 관련 신기술 등장 및 확산, 국제 규범 변화, 마이데이터 확산 등 시의성을 충분히 반영하기 어려워 로드맵 개정·고도화 필요

- 생성형·에이전틱·피지컬 AI 등 신기술의 급속한 확산과 국내 정책환경 변화 대응을 위하여 기 수립한 R&D 로드맵 보완이 필요한 상황

  - 특히, AI*는 새로운 분야로 정립하고, 향후 발전을 고려한 기술 R&D와 표준화 방향을 설정하여 개인정보의 침해·유출 위험*을 낮출 필요

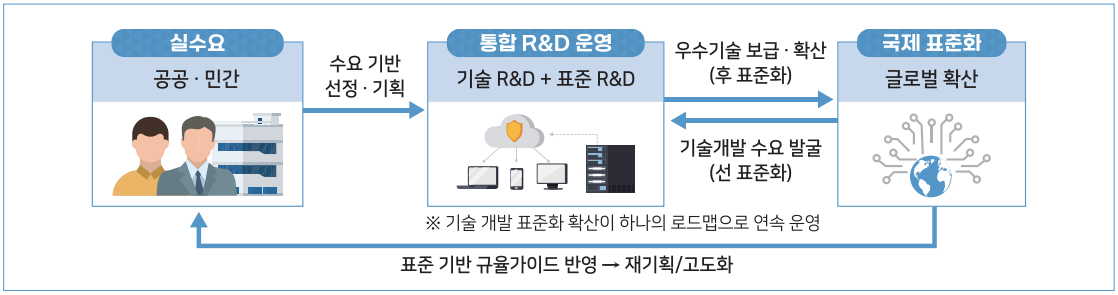
  * 의료·금융·공공 등 다양한 산업에서 고부가가치 데이터·AI 활용 수요가 급증하여, 프롬프트 공격·재식별·오남용 등 새로운 유형의 위험이 등장하는 상황

- 또한, 기술개발 성과가 글로벌 표준으로 이어질 수 있도록 종전의 표준화 로드맵('23~'27)과 하나로 통합·연계하여 체계적인 확산 추진

  - 이를 통해, 실수요 기반의 선도기술 선정 및 R&D를 추진하고, 구현된 기술이 글로벌 표준화까지 이어지는 선순환 체계 및 연속성 확보

※ 실수요자 기반의 기술개발 수요를 발굴하고, 우수기술을 보급·확산할 수 있도록 연계 강화

실수요 기반 '연구개발(R&D) ⇔ 표준화' 연계 체계



2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵

Ⅱ 국내 · 외 동향

1. 정책 동향
2. 산업 및 시장 동향
3. 기술 및 연구개발(R&D) 동향
4. 표준화 동향

CHAPTER II

국내 · 외 동향

1 정책 동향

(국내) 데이터의 핵심인 개인정보를 보호하고, 산업에서 안전하게 활용할 수 있는 R&D 추진 및 실증·확산을 통한 성과창출 추진

- 정보주체 권리보장, 아동·청소년·디지털 취약계층 보호, 침해 예방 조치 등에 필요한 개인정보보호 강화 기술(PET) 관련 R&D를 확대

  ※ 국민이 안심할 수 있는 개인정보 보호체계 확립 - 개인정보보호 강화 기술 R&D 확대(이재명 정부 국정운영 5개년 계획, '25.9월)

- AI 안전 분야와 관련, '딥페이크 탐지, AI 모델의 유해 콘텐츠 생성 차단 등' AI 오남용 대응 핵심기술 개발 및 상용화 지원

  ※ AI 안전 투자 강화, 데이터 개방, 융합 표준화, 인프라 구축 등 데이터 활용 확대(새정부 경제성장전략('25.8월))

- 향후, AI 관련 정책과 PET 연계가 강화되면서 가명처리, 재식별 방지 기술 등의 지속 수요가 증가할 것으로 예상

  ※「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」제정('26.1월)

  - AI와 데이터 활용에 대한 규제 관련 안내서 배포가 최우선 과제로 부상

(국내) 개인정보 보호·활용 관련 안내서

문서명	발간시기	기관	주요 목적 및 핵심 내용
생성형 AI 개발·활용을 위한 개인정보 처리 안내서	’25.08	개인정보위	· 공개된 개인정보를 안전하게 처리하는 방법 안내 · 데이터 수집 시 동의 절차, 비식별화 처리, 최소 활용 원칙 강조 · 활용 과정에서 법률 위반을 방지하기 위한 체크리스트 제공
합성데이터 생성·활용 안내서	’24.12	개인정보위	· 합성데이터를 생성·활용하는 기관을 대상으로 절차와 방법을 제시 · 데이터 생성 단계, 검증, 활용 절차를 세분화 · 재검토 주기를 3년으로 설정하여 지속적인 보완을 규정
AI 프라이버시 리스크 관리 모델	’24.12	개인정보위	· AI 프라이버시 리스크를 체계적으로 관리하기 위한 모델을 제시 · 리스크 요인을 식별하고 평가하는 프레임워크 제공 · AI 안전성, 투명성, 개인정보보호 원칙을 종합적으로 고려
합성데이터 생성 참조모델	’24.05	개인정보위	· 합성데이터 생성 과정을 표준화하기 위한 참조모델을 제안 · 단계별 절차와 평가 지표를 명확히 제시 · 산업에서 안정적으로 합성데이터를 생성·활용하기 위한 기반 마련
공공부문 초거대 AI 도입·활용 가이드라인	’24.04	행안부, 디지털플랫폼정부위	· 공공부문, 초거대 AI와 대규모 언어모델(LLM) 도입·활용 기준 제시 · 클라우드 서비스 연계 및 서비스 유형별 활용분류 제공 · 보안·윤리적 고려사항과 공공 책임성 확보를 위한 관리체계 제안
가명정보 처리 가이드라인	’24.02	개인정보위	· 가명정보 처리 절차와 안전조치 기준을 상세히 안내 · 가명처리 수준, 기술적·관리적 조치사항을 구체화 · 공공·민간 기관의 실무 적용을 위한 사례와 체크리스트 제공
신뢰할 수 있는 인공지능 개발안내서	’24.02	한국정보통신기술협회 (TTA)	· 인공지능 신뢰성 확보를 위한 산업별 개발 지침 제시 · 투명성·공정성·설명가능성 원칙 강조 · 데이터 품질과 환각 방지 조치 강조 · 도메인(일반, 생성형AI, 스마트치안 등) 별 위험요소와 대응 전략
금융분야 AI 개발·활용 안내서	’22.08	금융위, 금보원	· 금융기관이 AI를 개발·활용할 때 준수해야 할 기준 제시 · 데이터 보호조치, 신뢰성 검증, 내부통제 방안 제시 · 소비자 보호 및 금융보안 강화 목표

- AI 환경의 기술적 인프라와 보호를 위한 제도적 장치 마련을 병행하는 등 이중 전략(Two-track)을 중심으로 하여 연구보고서를 발간하는 추세

  - 개인정보의 보호·활용, 양 축을 충족하여 실질적인 정책효과로 나타나기 위해서는 'AI 인프라 확충, 보호제도 강화'를 동시 고려 필요

① 인프라 측면: GPU/AI반도체, 데이터센터, 공공·민간 AI 허브 구축

② 보호제도 측면: 데이터 최소 이용, 프라이버시 강화 기술(PET), 국제 규범 준수

☞ AI 인프라 확충과 함께 '보호·윤리 등 프라이버시 안전장치 내재화'가 전제

  - 국제적인 기술 체계*에 선제 대응하고, 국내 정책·기술개발과 표준화 연구 수행으로 안전한 기술적 대안을 마련하는 것이 중요

* 국제표준화기구(ISO/IEC), 경제협력개발기구(OECD), 국제전기전자공학회(IEEE) 등

(국내) 개인정보 보호·활용 관련 동향 보고서

보고서 명	발간시기	기관(출처)	주요 내용
제2차 국가연구개발 중장기 투자전략 ('26~'30) 수립방향	'26.01	과기정통부	· 핵심 AI 기반기술 개발로 확산·활용 가속화 · 기초연구 및 과학 육성 등 연구의 질 제고 · 중소·벤처, 인재, 지역 성장 등 연구생태계 혁신 · 재난·안전 대응, 사회문제 해결 등 튼튼한 사회구현
새정부 경제성장전략	'25.08	관계부처합동	· 데이터 안심구역 클라우드 전환 · 저위험가명데이터 개방 · 국가 AI 학습용 데이터 클러스터 및 데이터 스페이스 구축
이재명정부 국정운영 5개년 계획 (국정과제 25)	'25.08	국정기획위	· AI 학습용 원본정보 활용특례 도입 · 가명·익명정보 고도화, 개인정보보호 R&D 확대
AI DEEP INSIGHT '25-3: 가명정보제도 활성화 방안	'25.03	개인정보위	· 가명정보의 활용성 제고와 안전성을 동시 확보 · 재식별 위험 관리체계 강화 및 활용 촉진을 위한 법·제도 개선 필요성 제시
'25년 개인정보위 주요업무 추진계획	'25.01	개인정보위	· AI 시대 맞춤형 보호체계 고도화와 국제협력 강화 · 개인정보 관련 정책 집행의 우선순위 제시
'25년 정부혁신 실행계획	'25.01	개인정보위	· 개인정보 보호가 단순 규제가 아니라 정부 서비스 혁신의 필수조건 · 데이터 활용과 보호의 균형이 핵심 키워드
금융권 생성형 AI 활용 지원방안	'24.12	금융위	· 혁신 촉진과 소비자 보호·리스크 관리를 병행 필수 · 금융산업 특화된 안전망 마련 필요
국가AI전략 정책방향	'24.09	관계부처합동	· '민간 중심 AI 생태계 강화, 초거대 AI 경쟁력 확보, 인프라 확충'을 3대 축으로 정의 · 산업 전반에 AI를 전략적으로 확산하는 방향 제시

보고서 명	발간시기	기관(출처)	주요 내용
개인정보 보호 기본계획('24-'26)	'24.07	개인정보위	· 안전한 활용·가명/익명정보 촉진·국제협력 관련 정책 기조 표명 · 개인정보 보호와 안전한 활용 관점에서 정책제시
'24 개인정보보호 및 활용조사 보고서 /통계표	'24.06	개인정보위	· 국민과 기업의 데이터 활용 및 보호 인식 수준을 정량화 · 정책 수립을 위한 근거 제공, 사회 내 수용성 확인
'24 개인정보보호 연차보고서	'24.06	개인정보위	· 지난 1년간의 제도 성과·사건·법제 변화를 종합 · 정책 점검 및 계획의 연결고리 역할
'24 국가지능정보화 백서	'24.05	지능정보원	· 국가 AI 및 지능정보화 정책 전반을 총망라 · 공공·민간 AI 활용 현황·성과를 체계적으로 기록
인공지능 일상화 및 산업 고도화 계획(안)	'24.05	정부 합동	· AI의 생활 전반 확산과 산업 경쟁력 고도화 정책 목표로 설정 · 데이터·윤리·표준 등 다층 전략을 병행 필요
전국민 인공지능 일상화 실행계획	'24.04	과기정통부	· 국민이 체감하는 생활밀착형 AI 확산이 핵심 과제 · 산업 분야 전반에 걸친 AI 서비스 적용계획 수립
초거대AI 경쟁력 강화 방안	'24.04	과기정통부	· 초거대 AI 기술·산업의 선도권 확보를 목표 · R&D 투자, 인프라, 민·관 협력 강화로 경쟁력 확보

(국외) '아시아, 유럽연합(EU) 등'의 주요국은 AI를 국가전략 핵심 축으로 설정하고, '산업, 안보 등' 사회 전반에 걸쳐 생태계를 조성하는데 주력

- **(EU)** 초대형 컴퓨팅 인프라(기가팩토리*), 공통 데이터 공간, GenAI4EU** 산업 실증(의료·로봇·기후 등)을 강조

  * 기가팩토리: 초거대 AI 모델 학습·개발에 필요한 AI 연산자원과 운영(전력·냉각·보안 등)을 통합·제공하는 EU의 AI 컴퓨팅 인프라

  ** GenAIEU: 생성형 AI의 산업 적용·실증(use-case) 발굴·확산을 지원하는 EU 이니셔티브

  - 'EU AI Act, 영국 AI 규제 백서 등' 각 국 별로 규율체계를 마련하고 산업계 실증을 수행하는 등 'AI 생태계 전방위 확장' 전략*을 병행 추진

  * 약 2,000억 유로(€) 규모의 Invest AI와 AI Continental Plan 프로젝트 계획 추진

- **(미국)** '25년 美 행정부가 연방의 AI 관련 규제를 완화하고, 혁신과 경쟁력 강화를 위한 실행계획(180일) 수립·이행하는 행정명령 발표

  - 다만, 캘리포니아·뉴욕 등 일부 주(州)에서는 고위험 AI 규제, 투명성 확보 중심의 법제화 추진으로 고용·채용 등에 실무 적용 의무 강화

  ※ 美 연방에서는 규제완화 추세이나, 일부 주에서는 규제를 강화하는 등 상이한 정책 운용

  - National Science and Technology Council(NSTC)는 프라이버시 분야 연구전략으로 'AI와 데이터 분석 시 위험 저감, PET의 내재화, 데이터 투명성 강화 등' 보호·활용의 동시 달성을 위한 국가 R&D 방향 제시

  ※「National Privacy Research Strategy」('25): 「프라이버시 보호형 데이터 공유·분석 촉진 국가전략(PPDSA, '23)」 등을 보완하고, AI 기술 확산에 따른 PET 중심 연구개발 의제를 구체화

- **(영국·싱가포르)** PET와 데이터 보호에 관한 실무 안내서 등을 마련하여 실증 등을 수행하는 추세

  - **(영국)** 공공·금융·의료에서의 PET 적용 가이드 발간으로 데이터 공유·활용을 위한 실무 기준 등을 안내

  - **(싱가포르)** PET 샌드박스와 관련 안내서, AI 기술의 신뢰성 검증용 도구(Toolkit)를 통하여 민간 실증과 신뢰성 확인 등 병행

  ※ 산업 현장의 여건에 맞추어 실무 과정에서 PET를 어떻게 적용·검증할지 초점

- **(동북아)** AI를 국가의 핵심 전략산업으로 설정하고, '산업, 안보' 등 사회 전반에 변화를 일으키는 국가 전략형 AI 정책을 추진

  - **(중국)** AI를 국가안보와 산업 경쟁력의 중심 전략으로 채택

  - **(일본)** 민·관·연 등과 협력 및 현장에서 실증과 사회적 수용성을 높여 국제 규범과의 정합성도 함께 강화해 나아가는 정책 수립

  ※ 신뢰가능한 AI 활용을 위한 기준과 운영원칙 등을 마련

(국외) 개인정보 활용에 필요한 PET 적용 정책 주요내용

국가	문서 명	발간시기	기관(출처)	주요 내용
유럽 연합 (EU)	InvestAI Initiative	'25.02	EU 집행위	· 2,000억 유로 투자 동원 · 4대 AI 기가팩토리·데이터 공간·GenAI4EU 산업 실증 추진 · EU 전역 AI 생태계 강화, 산업 경쟁력 제고
	AI Continental Plan (EU 대륙 실행계획)	'25.04	EU	· EU 내 AI 실행전략 세부 로드맵 제시 · AI 인프라·데이터·산업 실증 확대 · 교육·역량강화와 기업 지원 병행 · 유럽형 책임있는 AI 프레임워크 구축
미국 (연방)	트럼프 행정부 행정명령 (Removing barriers to AI leadership)	'25.01	백악관	· 바이든 정부의 AI 규제 행정명령 철회 · 180일 내 실행계획 수립 지시 · 규제 완화와 미국 우위 확보 기조 강화
	AI 액션플랜 (트럼프 행정부)	'25.02 ~06	NIA 분석 (Deep Insight, The LENS)	· 규제완화·산업계 중심 정책 기조 · 국가 AI 경쟁력 확보 우선 · 산업계 제언을 반영한 실행방안 수립 · '신뢰성·윤리' 중심으로 정책 대전환
미국 (주별)	AI Governance & Law	'25.05	주별 입법(콜로라도·캘리포니아·뉴욕 등)	· 고위험 AI 규제와 자동화 의사결정 거부권 도입 · 투명성 법제화 및 차별 방지 조치 · 주(州) 별로 차등 규제와 기업의 자율적인 거버넌스 운용 병행
미국 (표준)	NIST Privacy Framework 1.1 Draft	'25.01	NIST	· 사이버보안 프레임워크(CSF) 2.0 가이드라인과 정합성 강화 · PET 및 데이터 보호 기술 반영 · 국가 프레임워크의 최신화와 산업 적용성 확대
미국 (전략)	National Privacy Research Strategy	'25.01	NSTC	· AI활용·데이터 분석 시 프라이버시 위험 저감 방향 제시 · PET 고도화와 프라이버시 평가 연구 강화 · 연방기관 간 프라이버시 R&D 협력 추진
영국	ICO PET Guide	'25.01	ICO	· 공공·금융·의료 분야 PET 실무 가이드 · 데이터 공유·활용 시 PET 적용 사례 제시 · PET 도입의 실무적 기준 제시
싱가포르	PET Sandbox & PET Adoption Guide	'25.01	IMDA/PDPC	· PET 도입을 위한 샌드박스운영 · AI 신뢰성 도구 세트 공개 · 민간 도입 촉진과 신뢰성 확보 기술 실증
일본	AI 제도 기본방침(안)	'25.05	정부	· 책임있는 AI 개발과 사회적 수용성 확보 · 산업계와 학계 협력 통한 활용 촉진 · 국제 규율체계 연계, 동아시아 리더십 확보 · AI 윤리·법제 정합성 고도화
중국	'25 양회 정부업무 보고	'25.03	정부	· 디지털 경제 강화 · 산업·안보·사회 전반 AI 통합 · 국가안보와 산업 경쟁력 중심 AI 정책
프랑스	Make France an AI Powerhouse	'24~'25	정부	· AI 연구역량 강화 및 AI 산업 인프라(컴퓨팅·데이터센터) 확대 · 규제와 혁신의 균형에 중점 · AI 국가 경쟁력 확보 및 EU 리더십 강화

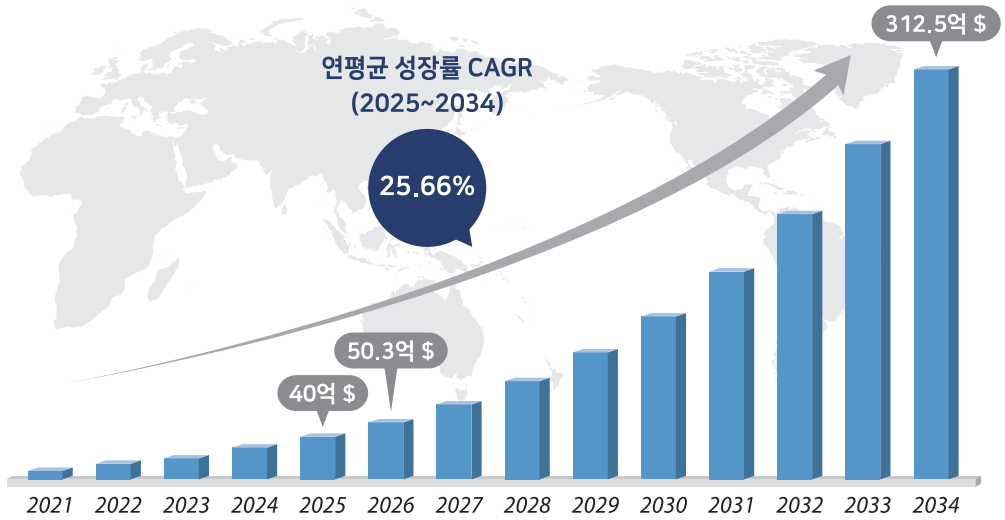
2 산업 및 시장 동향

(전 세계 PET 시장) 글로벌 리서치 기업의 PET 시장 규모 및 전망[1] 에 따르면 전 세계 시장 규모는 '34년까지 약 312억 달러(매년 약 25.6% 성장) 예상

※ ('26년) 50억 3천만 달러(한화로 7.5조원) → ('34년) 312억 5천만 달러(약 47조원) 규모

- 특히, '개인정보보호 중심 설계(PbD) 내재화, AI와 PET 결합, 클라우드 기반 PET 기술 등'의 확산으로 PET 관련 시장·보호기술 수요가 큰 폭으로 증가

※ PET는 신기술과 융합되어 활용과정에서 개인정보 보호가 동시 달성 가능한 핵심기술로 주목



※ 출처: Privacy Enhancing Technologies Market Size, 2021-2034(Fortune Business Insights, '26.3월)

- 한편, 국내 PET 시장 규모는 '26년 2,938억원에서 '34년에는 약 1조 8,265억 원까지 매해 성장할 것으로 예측

※ (산출 근거) '26년 국내 PET 시장 추정치 2,214억~2,938억 원

>> 국내 정보보안('23) 6.145조 원 × 글로벌 PET 비중(1.9-2.5%) 반영

>> (성장률, CAGR) 글로벌 PET 시장 연평균 성장률(CAGR)은 25.66%로 예측

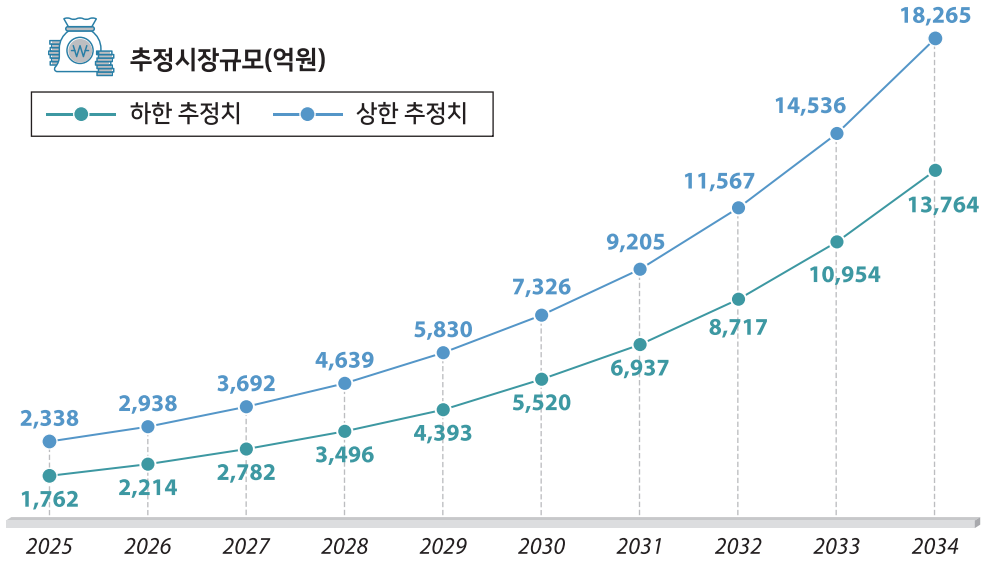
※ 출처: Fortune Business Insights, Privacy Enhancing Technologies Market Size, Share, Trend 2034

>> (적용 방식) 하한: 2,214억 원 × (1.2566^8), 상한: 2,938억 원 × (1.2566^8)

>> 이에 따라 '34년 국내 PET 시장은 약 1조 3,764억~1조 8,265억 원 규모로 추정됨

1) Privacy Enhancing Technologies Market Size, Share, Trend 2034, https://www.fortunebusinessinsight.com/

국내 PET 시장 규모


추정시장규모(억원)
하한 추정치
상한 추정치
2,338
2,938
3,692
4,639
5,830
7,326
9,205
11,567
14,536
18,265
1,762
2,214
2,782
3,496
4,393
5,520
6,937
8,717
10,954
13,764
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034

(산업 동향) 단일 PET 기술의 한계를 보완할 수 있도록 상호 보완적인 PET 기술을 조합하여, 개인정보 유·노출 위험도를 낮추는 환경으로 진화

- **(글로벌 빅테크)** 연합학습·차분프라이버시·동형암호 등을 융합하여 자사 플랫폼에 내재화하는 등 'PET as a Service' 생태계 주도
- **(스타트업)** 합성데이터·동형암호·다자간 연산 등 PET 기술을 금융·헬스케어 등 산업에 특화하여 고부가가치 시장을 선점하는 데 주력

(국외) PET 관련 산업 동향

기술 분야	주요 기업	주요 내용
연합학습 + 차분 프라이버시	A사	· Gboard에 연합학습과 차분 프라이버시가 동시 적용된 상용 모델 운영 · '24년부터 모든 Gboard 다음 단어 예측 모델에 차분 프라이버시 기술 적용 · Formal DP 보장을 충족하는 첫 상용 신경망 모델을 비영어권 국가의 Gboard에 적용
연합분석 + 차분 프라이버시	B사	· iOS 분석 데이터 수집 과정에 차분 프라이버시를 내장 · 연합 분석 개념을 도입하여 중앙 분석 서버 내 사용자의 원본 데이터 미저장 및 프라이버시 보존형 분석을 수행
기밀 컴퓨팅·안전한 다자 연산·동형암호	C·D사	· 하드웨어 기반 기밀 컴퓨팅(신뢰받는 실행 환경)을 통해 클라우드 내 민감 데이터 분석을 지원 · 다자간 연산·동형암호 기반 분석 서비스를 금융·헬스케어 등에서 개념 검증(PoC)을 수행하며, 안전한 데이터 공유·연산 구조 제시
데이터 클린룸	E사	· 기업 간 데이터 공유·분석을 위한 PET as a Service(SaaS형) 환경의 클린룸 서비스 제공 · 광고·마케팅, 금융 거래 데이터 협업 등에서 원시 데이터 노출없이 결합·집계·분석이 가능하도록 PET 기능을 서비스 형태로 제공
합성데이터	F사	· 정형(테이블) 데이터 기반 합성데이터 생성 플랫폼 솔루션 제공 · 유럽 GDPR 요구사항을 반영한 개인정보 보호형 합성데이터 생성 기술로 금융·보험 등 다양한 산업에 솔루션 공급
합성데이터	G사	· 개발자 친화적 API·플랫폼을 제공하는 합성데이터 스타트업 · 다양한 산업군(금융, 제조, 헬스케어 등)에 대한 실증 프로젝트를 통해 데이터 공유·학습용 합성데이터 제공
합성데이터	H사	· 의료 영상, 위성·원격탐사 데이터 등 고위험·고가치 데이터에 특화된 합성데이터 생성 및 분석 플랫폼 제공 · AI 모델 학습용 대규모 합성 이미지·영상 데이터셋 구축
암호화 + 안전한 다자 연산	I사	· 동형암호와 다자간 연산을 결합한 보안 분석 플랫폼 제공 · 금융기관·기업 간 민감 데이터를 직접 공유하지 않고도 공동으로 분석·모델링을 수행할 수 있는 협업·분석 환경 지원
블록체인 + 안전한 다자 연산	J사	· 블록체인과 MPC를 결합한 데이터 교환·스마트 계약 플랫폼 제공 · 프라이버시 보호형 데이터 마켓·데이터 교환 서비스 구현에 활용
동형암호	K사	· 오픈소스 동형암호 라이브러리를 제공하고, 동형암호를 AI 학습·추론 모델에 적용하는 연구·실증을 진행 · 개발자가 동형암호 기반으로 PET 활용이 용이하도록 전용도구·SDK 제공

- **(국내)** 다양한 PET 솔루션이 의료·금융 중심으로 빠르게 확산 중
  - 일부 기업은 글로벌 수준의 개인정보 보호·활용 기술을 적용하여 서비스로 운영 중

(국내) PET 산업 동향

기술 분야	주요 기업	주요 내용
연합학습(FL)	L사	· 병원 간 환자 데이터 외부 반출 없이 안전하게 AI 학습 가능한 연합학습 플랫폼 제공
합성데이터	M사	· 도메인 특화 합성 AI 데이터 솔루션으로 국방·자율주행·보안 등 다양한 산업군에 적용
합성데이터, 차분 프라이버시	O사	· 차분프라이버시(DP) 기반 노코드(No-Code) 합성데이터 플랫폼
동형암호	P사	· 4.5세대 동형암호 엔진: 근사 동형암호(Cheon-Kim-Kim-Song, CKKS) 기반의 근사(실수) 연산 지원 동형암호 엔진 · ES2(Encrypted Similarity Search) 솔루션으로 실시간 암호문 상태에서 검색 기능 지원
동형암호, 차분 프라이버시	Q사	· 동형암호와 차분 프라이버시가 융합된 PET 기반 솔루션 · 완전동형암호(Fully HE, FHE) 기반의 오픈소스 라이브러리로 다중 GPU 환경 최적화를 통해 기존 대비 연산속도 200배 향상
		· 차분 프라이버시 기술 포함 데이터 클린룸(CleanRoom) 솔루션
차분 프라이버시	R사	· 가명·익명 처리 시스템, 대용량 분산 가명처리, 차분 프라이버시 메커니즘 포함

3 기술 및 연구개발 (R&D) 동향

국내·외 기술 동향

- **(국외)** PET는 개인정보를 공개하지 않은 상태에서 연산·분석을 수행할 수 있는 기술로써 실 서비스에 탑재하여 상용화하는 추세
  - 경제개발협력기구(OECD)에서는 PET를 '개인정보 수집, 가공, 처리, 분석, 제공 등' 기술적 특성에 따라 유형을 구분

(국외) 기술 유형 별 주요 PET 분류

구 분	PET	개 념
데이터 난독 처리 (Data Obfuscation)	차분 프라이버시 (Differential Privacy, DP)	· 데이터 세트에 노이즈를 추가하여 분석 결과를 도출함으로써, 해당 분석결과로부터 특정 개인을 역으로 추론하지 못하도록 하는 기술
	합성데이터 생성 (Synthetic Data Generation, SDG)	· 실제 데이터의 중요한 통계적 특성을 활용하여 생성한 가상의 데이터 세트를 실제 데이터 대신 활용
	영지식 증명 (Zero Knowledge Proofs, ZKP)	· 자신의 정보 내용 자체를 전달하거나 노출하지 않고도 자신이 그 정보를 알고 있다는 사실을 참·거짓으로 증명
암호화된 개인정보 처리 (Advances in Cryptography)	동형 암호화 (Homomorphic Encryption, HE)	· 일반 텍스트를 공개하지 않고, 암호화된 데이터의 연산 수행
	신원 기반 암호화 (Identity-Based Encryption, IBE)	· 전통적인 공개키 인프라 대신 개인 키 생성을 통해 발신자에서 수신자 방향의 메시지에 암호화 적용
	안전한 다자 연산 (Secure Multi-Party Computation, SMPC)	· 암호화된 여러 데이터에서 다른 사람들에게 개인 데이터를 공개하지 않고도 관심값(values of interest)을 계산할 수 있는 분산 컴퓨팅 시스템 또는 기술
	신뢰받는 실행 환경 (Trusted Execution Environment, TEE)	· 운영체제(OS)에서 독립적인 CPU 내부 하드웨어의 보안 영역이며, 이 영역에 개인정보를 보관하여 기밀성을 유지한 상태에서 연산 수행
연합 및 분산 분석 (Federated and Distributed Analytics)	연합학습 (Federated Learning, FL)	· 참여자가 로컬에서 기계학습 모델 훈련에 참여함으로써 학습 데이터를 기기 내 유지하고, 요약 데이터만 중앙 데이터 저장소에 전송할 수 있도록 허용
	분산분석 (Distributed Analytics, DA)	· 분산된 데이터에 대하여 분석·통계 처리를 위한 기술이며, 데이터 간 이동없이 분석 결과를 수신
데이터 거버넌스 도구 (Data Accountability Tools)	책임 시스템 (Accountable Systems)	· 데이터를 다루는 전 과정에서 거버넌스 차원으로 투명성·추적성·책임성을 확보하기 위한 관리적·기술적 체계
	개인정보 관리 시스템 (Personal Information Management Systems)	· 개인 데이터 저장소(Personal Data Storage, PDS) 등과 같이 정보주체에게 자신의 개인정보에 대한 통제권 제공

※ 출처: EMERGING PRIVACY ENHANCING TECHNOLOGIES (OECD DIGITAL ECONOMY PAPERS, 2023)

- 특히, '미국, 유럽 등' 주요국의 공공기관에서는 PET를 개인정보를 목적에 맞게 안전하게 처리하여 활용 중

주요 기관의 PET 활용 사례

PET	기관	목적	활용 데이터
안전한 다자 연산 (SMPC)	미국 보스턴 여성노동자협의회	안전한 다자간 계산을 활용해 급여 격차 측정	· 보스턴의 성별 및 인종 간 임금 격차
	유럽 통계 시스템	스마트 설문조사 기술 개발	· 참여자의 기기에서 수집된 센서 데이터
	미국 교육부	개인정보보호 기록 연계를 이용한 학생 재정지원 데이터 분석	· 학부생의 평균 학자금 대출 및 보조금 데이터
신뢰받는 실행환경 (TEE)	유럽연합 통계청 - Eurostat	모바일 네트워크 사업자의 데이터 처리	· 통화기록, 가입자의 방문 위치 등
	인도네시아 관광부	두 모바일 사업자의 데이터를 공유 및 결합해 통계 생성	· 망사업자의 IMSI 목록
동형암호 (HE)	캐나다 통계청	암호화를 통해 기계학습을 위한 개인정보 분류	· 개인정보 정형데이터(텍스트)
합성데이터 생성 (SDG)	캐나다 통계청	합성데이터 활용 검증 및 테스트	· 교육 및 해커톤을 위한 고품질 데이터
차분 프라이버시 (DP)	미국 인구조사국	인구조사에서 수집한 민감정보의 노출 방지	· 미국 인구조사 관련 데이터
안전한 다자 연산 동형암호, 차분 프라이버시 (SMPC, HE, DP)	대한민국 국가데이터처	개인정보보호 통계 데이터 허브 플랫폼 개발	· 다양한 종류의 통계 데이터
안전한 다자 연산, 동형암호, 연합학습 (SMPC, HE, FL)	이탈리아 통계청 및 은행	양 기관의 개인정보를 연결해 데이터 분석	· 인구통계 및 금융 데이터 셋
	네덜란드 통계청	분산된 임상 등의 데이터를 토대로 개인정보를 보호하는 환경 하에서 심혈관 위험 예측 모델 개발	· 1·2차 병원의 임상시험 결과 데이터 셋
연합학습, 동형암호, 차분 프라이버시 (FL, HE, DP)	UN 유럽 경제위원회	스마트 기기에서 수집한 개인의 일상습관 관련 데이터를 이용하여 기계학습 모델 개발	· 스마트장치(Device)에서 수집된 데이터 셋
안전한 다자 연산, 차분 프라이버시 (SMPC, DP)	UN PET Lab	여러 국가 통계청에서 수집된 데이터 분석	· UN Comtrade 데이터 셋에서 수집한 데이터

• **(국내)** 공공·금융·의료분야에서 실증환경에서 주로 PET를 활용 중이며, 솔루션 등 상용화를 통해 시장으로 보급하기 위한 노력을 지속 중

- 합성데이터 생성 솔루션, 연합학습 기반의 의료 데이터 분석 등 국내 활용 사례가 점차 등장

※ 미국 등 선진국 대비 국내 PET 적용은 실증·활용 확산 측면에서 아직 초기 단계수준

- 공공·금융·의료 중심으로 활용이 확대되는 가운데 정부 주도의 연구개발 외에도 민간 투자가 점차 확대되는 추세*

* 2024 개인정보 이슈 심층보고서(Vol.2) (한국인터넷진흥원, '24.7월)

(국내) 주요 기관의 PET 활용 사례

PET	기관	목적	활용 데이터
신뢰받는 실행환경 (TEE)	국가데이터처	개인정보 포함 데이터를 개인정보 이노베이션 존에서 안전하게 처리	· 통계 데이터센터 반입·분석 데이터
합성데이터 (SDG)	개인정보위	합성데이터의 안전한 생성·검증·활용 절차 및 적용 사례 등 제시	· 정형·비정형 합성데이터에 필요한 참조 모델 제작·배포로 안전한 활용 기반 제공
연합학습 (FL)	복지부	멀티모달 연합학습 기반 의료용 AI 기술 시범모델 연구개발 시, 다수의 의료기관이 데이터 반출 없이 학습·실증을 위한 목적	· 의료기관 별로 각기 보유한 전자의무기록(EMR) 등 의료 데이터
연합학습 (FL)	복지부	제약·바이오 영역에서 신약개발용 AI 모델 연구개발에 활용	· 각 기관·기업이 보유한 신약개발에 필요한 개인정보 등 데이터
동형암호 (HE)	중기부	동형암호 기반으로 암호화 상태에서 분석 가능한 데이터 클린룸 운영 (혁신제품 지정·공공조달 연계)	· 암호화된 민감데이터를 복호화 없이 분석·처리 가능

연구개발(R&D) 동향

- **(국외)** 데이터 경제의 핵심 인프라로 PET를 적용하는 기술 전략을 추진
  - **(미국·영국)** '동형암호, 연합학습 등'을 활용한 프라이버시 보존형 데이터 분석 기법을 실증*하는 데 주력하고 있는 상황

  * 개인정보보호 강화 기술 경진대회(U.S.-U.K. PET Prize Challenge): 영국 데이터윤리·혁신센터, 미국 백악관 과학기술정책실 등이 공동 주최하는 대회로, '자금세탁방지, 팬데믹 대응 분야'에 PET를 적용

  - **(EU)** Horizon Europe*을 통해 헬스·에너지·제조 등 영역 별 데이터에 대하여 차분 프라이버시, 합성데이터 등 PET 활용을 통한 실증 추진

  * EU의 '핵심 연구·혁신(R&I) 재정 프로그램'(예산 약 955억 유로 규모, '21~'27)'민·관·연 및 학계가 참여하는 공동 연구, 실증, 표준·정책 연계 등'을 포괄하는 지원 프로그램

  - **(OECD)** PET 기술 분류 정의와 함께, 관련 기술의 성숙도 평가 기준을 마련하여, 각 국의 규율체계와 R&D가 연계 가능한 가이드라인*을 제시

  * 「Emerging privacy-enhancing technologies: Current regulatory and policy approaches」(OECD Digital Economy Papers No. 351)「Sharing trustworthy AI models with privacy-enhancing technologies」(OECD Artificial Intelligence Papers No. 38) 등

  - **(기술 규격화)** PET 관련 용어·참조 아키텍처·기술 규격을 국제 표준화*하는 등 범용성 있는 상호운용성과 인증체계를 마련 중

  * 국제 표준화기구(ISO/IEC), 유럽전기통신표준협회(ETSI), 국제전기통신연합(ITU-T)에서 프라이버시 관련 표준화 활동을 진행 중

- **(국내)** 정부의 지원을 통해 '연구·국제표준화→실증→민간'으로 이어지는 선순환 구조 조성을 위하여 PET의 단계적 확산을 추진 중
  - 개인정보위는 개인정보를 보호하고, 안전하게 활용할 수 있도록 R&D 사업 매년 확대해 나가는 등 국제수준의 PET 선도기술 개발을 추진 중

  ※ '22년 첫 R&D 사업 시작 후, '26년에는 약 4.5배 예산이 증액 / ('22) 30억원 → ('26) 132억원

  - 특히, AI 환경에 적합한 기술 연구를 통해 산업 등에서 활발히 활용할 수 있도록 실수요 기반의 기술·표준 R&D* 환경 및 생태계 조성에 노력

  * AI 학습데이터의 안전성 검증 기술, 실시간 딥페이크 방지 기술, 가명정보 및 합성데이터 생성·활용 기술 등 실 환경에서 적용 가능한 선도기술 연구에 집중

4 표준화 동향

국외 표준화 동향

- **(ISO/IEC)** 개인정보 보호·활용 관련 글로벌 표준 체계로 확장·고도화하여 나아가는 추세

※ 국제표준화기구/국제전기기술위원회(ISO/IEC) 내 IT 공동기술위원회 제27분과 위원회(JTC1 SC27) 운영

- 프라이버시에 특화된 프레임워크·영향평가·위험관리 체계를 개정('22년~)

※ ISO/IEC 29100:'11(Privacy framework, '24), 29134:'17(Privacy Impact Assessment, '23,), 27557:'22(Privacy risk management), 29151:'17(Code of practice for personally identifiable information protection) 등

- 데이터 비식별화 및 동의 이력 관리 표준을 통해 데이터 활용과 정보주체 권리보호 간 균형을 확보

※ ISO/IEC 20889:'18(De-identification terminology), 27559:'22(De-identification framework), 27560:'23 (Consent record information structure) 등

- 향후, AI·플랫폼 환경을 고려한 신규 프라이버시 표준이 순차적으로 제정·발간될 예정

※ ISO/IEC 27566:'25(Age assurance systems), 27564:'25(Guidance on the use of models for privacy engineering), DIS 28033-1:(예정)(Fully homomorphic encryption Part 1: General) 등

- **(ITU-T)** 통신·네트워크 환경에 필요한 개인정보 보호 관련 표준을 주로 진행하며, 최근 클라우드·모바일·생체인증·인증 환경까지 확대

- 개인식별정보(PII) 보호 코드와 연계하여, 생체정보 보호, 온라인 인증, 망·클라우드 환경에서의 개인정보보호 기준을 구체화

※ 국제전기통신연합ITU-T): D.1141:'25.04(Policy framework and principles for data protection in the context of big data related to telecommunication/information and communication technology services), X.1647:'24.10(Security guidelines for selecting computing methods and resources from cloud service providers) 등

- AI 프라이버시 환경에서 적용이 가능하도록 차세대 서비스 시나리오를 제시하기 위한 개정·신규 표준 논의 진행

- **(NIST)** Privacy Framework('20)를 토대로 개인정보에 대한 비식별화·차분프라이버시 관련 기술 지침(가이드)과 거버넌스 체계를 지속 강화

- 개인정보에 대한 비식별화, 차분프라이버시한 관련한 문서* 발간

* 국립표준기술국(NIST): 800-226(Guidelines for Evaluating Differential Privacy Guarantees, '25.3), SP 800-188(De-identifying Government Datasets, '23.9), IR 8053(De-identification of Personal Information, '15.10) 등

- 개인정보 보호와 AI 거버넌스·신뢰성 관리를 통합·연계*하는 추세

* NIST Privacy Framework v1.0/1.1과 AI Risk Management Framework(AI RMF, '23) 연계

국내 표준화 동향

- **(한국정보통신기술협회(TTA))** 가명·익명처리, 동형암호, 분산형 ID(DID), 생체인증, 개인정보 영향평가(PIA), 접근통제 등으로 표준화 범위를 확대 중
  - 개인정보 처리 관련, '안내·고지 동의 등' 정보주체 권리보호에 필요한 세부 표준사항들은 표준화로 제정해 나아갈 필요

- **(한국산업표준(KS))** ISO/IEC 국제표준 중 일부를 채택·적용 중이며, 국내 환경에 적용 및 응용 가능한 표준화 작업은 지속적으로 필요

국내·외 표준 제정 목록(최근 10년)

* 최신 제정 연도 순

구분		연도	표준 번호	제목 / 내용(요약)
국내	KS	'23	KS X ISO/IEC 29100	· 정보기술·보안기술·프라이버시 프레임워크 - ISO/IEC 29100:2024 프레임워크를 국내 채택
	TTA	'22	TTAK.KO-10.1410	· 빅데이터 유통 플랫폼 - 정형 데이터 비식별 조치 기능 요구사항
	KS	'22	KS X ISO/IEC 27701	· 정보보안·사이버보안 및 프라이버시 보호 – 개인정보보호 정보관리 시스템(PIMS) 요구사항 및 안내 - 국내 PIMS 인증제도의 요구사항과 실행지침을 제공 - KS X ISO/IEC 27001과 27002 기반의 확장된 표준
국외	ISO/IEC	'25	ISO/IEC 27566-1	· Information security, cybersecurity and privacy protection-Age assurance systems - Part 1: Framework(연령 확인 시스템 프레임워크)
	NIST	'25	SP 800-226	· Guidelines for Evaluating Differential Privacy Guarantees - 차분 프라이버시 기술의 보증(Guarantee)을 위한 평가 지침
	NIST	'25	NIST Privacy Framework v1.1(IPD)	· Privacy Framework 1.1(Initial Public Draft 진행 중) - 개인정보 처리과정에서 발생할 수 있는 프라이버시 위험을 관리하기 위한 프레임워크
	ISO/IEC	'24	ISO/IEC 29100	· Information technology-Security techniques-Privacy framework - 개인정보 처리시스템을 설계, 구현, 운영할 때 고려해야하는 기본원칙 제시
	NIST	'23	SP 800-188	· De-Identifying Government Datasets: Techniques and Governance(정부 데이터셋 비식별화 기술·거버넌스) - 정부 데이터 비식별화 기법 및 거버넌스 공개 절차 제시
	ISO/IEC	'23	ISO/IEC 27560	· Consent record information structure(동의 기록 정보 구조) - 동의 기록 정보구조 표준화 및 동의정보 교환 방식 정의
	ISO/IEC	'23	ISO/IEC 29134	· Guidelines for privacy impact assessments(PIA 절차 및 보고서 구조 가이드라인) - 개인정보영향평가 절차 및 보고서 구성·필수항목 제시

구분		연도	표준 번호	제목 / 내용(요약)
국외	NIST	‘22	SP 800-53A Rev.5	· Assessing Security and Privacy Controls in Information Systems and Organizations(보안·프라이버시 통제 평가 절차) - 보안·프라이버시 통제 평가 절차 방법론 제공
	ISO/IEC	‘22	ISO/IEC 27559	· Privacy enhancing data de-identification framework(데이터 비식별화 프레임워크) - 데이터 비식별화 생애주기 위험 식별 및 완화 관련 프레임워크
	ISO/IEC	‘22	ISO/IEC 27557	· Application of ISO 31000:2018 for organizational privacy risk management(조직 프라이버시 위험관리 프레임워크) - ISO 31000 기반 조직 프라이버시 위험관리 절차 안내
	NIST	‘20	NIST Privacy Framework v1.0	· A Tool for Improving Privacy through Enterprise Risk Management (프라이버시 프레임워크 1.0) - 조직 위험관리 관점의 프라이버시 위험관리 프레임워크
	NIST	‘20	SP 800-53 Rev.5	· Security and Privacy Controls for Information Systems and Organizations(보안·프라이버시 통제 카탈로그) - 프라이버시 등 통제 목록 제공 및 통제 선정 기준 제시
	NIST	‘20	SP 800-53B	· Control Baselines for Information Systems and Organizations (통제 베이스라인 세트) - 영향도 별 프라이버시 통제 베이스라인 및 적용지침 등 정의
	ISO/IEC	‘20	ISO/IEC 29184	· Information technology — Privacy notices and consent(온라인 프라이버시 고지·동의) - 온라인 고지·동의 구성요소 및 절차 표준 규정
	ISO/IEC	‘19	ISO/IEC 27701	· Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management(PIMS 국제표준) - 개인정보보호 관리체계(PIMS) 요구사항 및 통제지침 정의
	ISO/IEC	‘18	ISO/IEC 20889	· Privacy enhancing data de-identification - Terminology and classification of techniques(비식별화 용어·기법 분류) - 비식별화 용어 정의 및 기법 분류 기준 제시
	NIST	‘17	NISTIR 8062	· An Introduction to Privacy Engineering and Risk Management in Federal Systems(프라이버시 엔지니어링·위험관리 개요) - 프라이버시 엔지니어링·위험관리 개념 및 접근방법 소개
	ITU-T ISO/IEC	‘17	ITU-T X.1058 (ISO/IEC 29151)	· Code of practice for personally identifiable information protection (PII 보호 실무 통제·가이드) - 개인정보보호 통제목표·및 구현 가이드라인 제시
	NIST	‘15	NISTIR 8053	· De-identification of Personal Information(개인정보 비식별화 지침) - 개인정보 비식별화 용어·절차·기법에 대한 기본 지침 제공

2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵

Ⅲ 추진방향

1. 정책 · 시장 및 기술동향 분석
2. 국내 개인정보 R&D 현황 분석
3. 개인정보 R&D 비전 및 추진방안

CHAPTER
Ⅲ

추진방향

1 정책·시장 및 기술동향 분석

AI 확산으로 개인정보의 안전한 활용에 필요한 기술 수요 증가

- 데이터 경제·생성형 AI 확산으로 개인정보 생애주기 전 과정에서 PET 적용 범위가 확대
- SNS·비대면 서비스·IoT·로봇 등의 보급으로 인한 비정형·멀티모달 데이터의 급증
- 대규모 언어 모델(LLM), 에이전틱·피지컬 AI 등에 대한 학습용 데이터의 개인정보 비식별 처리와 프라이버시 보호기술 수요 증가
- '연합학습+차분 프라이버시, 동형암호+안전한 다자 연산' 등 융합형 PET를 개발하는 국제적인 추세에 따라 관련 R&D를 국내에 확대 필요

  ※ PET가 AI 모델 공유·배포·학습 협업의 핵심 인프라임을 강조(EU, OECD, 사이버보안기구(ENISA) 등)

- 개인정보 오남용·침해 위협에 대한 국민 불안해소와 AI 서비스의 프라이버시 신뢰확보 요구 증가

  ※ AI 서비스 전 주기에서 프라이버시를 보장하는 PET-AI 융합 기술 개발 시급

법 제도·정책 변화에 대응하는 프라이버시 기술 확보 필요

- 국내 개인정보보호법 개정과 EU GDPR·AI Act, 각국 데이터 법 등 글로벌 규제가 강화되는 추세에 대응하는 기술 확보가 중요
- 국내에서는 전 분야 마이데이터, 공공·통계 데이터 등에서 가명정보·합성데이터 활용을 위한 제도가 활성화되는 추세
  - 신기술에 부합하는 프라이버시 기술 개발을 통해 개인정보를 안전하게 처리하여 제도적으로 뒷받침할 수 있도록 지원 필요
- 상시적인 프라이버시 내재화를 위한 전문적인 PET 기술 개발 필요
  - 개인정보보호 중심 설계(PbD)를 통해 시스템 및 데이터 처리 전 과정에 프라이버시를 내재화하는 기술을 적용하여 국민의 신뢰 확보

산업별 수요를 반영한 국제수준의 AI 친화형 PET 개발 및 표준화 연계 필요

- 글로벌 기업들은 서비스 내 PET를 내장(Embedded PET)하는 전략 추진 중

  ※ 모바일/헬스케어 서비스에 연합학습·차분 프라이버시 내재화, 데이터 클린룸, 실증 확대 등

- 그래픽처리장치(GPU)·신경망처리장치(NPU)의 가속·경량화 알고리즘 등을 활용한 고성능·저비용 PET 엔진 개발이 핵심 기술력으로 부각

  - 특히, 최적화된 융합형 PET* 적용을 위해, '보안성, 정확도, 연산비용' 등을 종합적으로 고려하여 개발 필요

  * 동형암호, 안전한 다자 연산, 연합학습, 합성데이터 등 수요에 맞는 PET 융합·적용

- 다만, 국내에는 산업 별로 적용 가능한 AI-PET 기술은 초기 단계

  ※ 자금세탁방지(AML)/고객확인제도(KYC) 신용평가, 병원 간 데이터 결합·AI 진단, 공공데이터의 합성데이터 등에서 활용

  - 국내 기업이 글로벌 시장에 진입하기 위해서는 국제표준과 호환 가능한 기술 개발 등이 필요

  ※ EU ENISA, OECD, 싱가포르 정보통신미디어개발청(IMDA) 등에서는 데이터 스페이스*·샌드박스 실증 시에 표준 및 상호운용성(Interoperability)을 필수사항으로 점검

  * 데이터 스페이스: 기관·기업 간 활용 조건 등 공통 규칙과 호환 방식 등 표준을 정의하여, 개인정보 등 보호가 필요한 데이터를 안전하게 공유·연계·활용하는 환경

종합 시사점

- AI 시대에 부합하는 개인정보 보호 및 생애 전 주기 별 안전한 활용을 위한 PET 개발 추진

  - 특히, 학습·추론·협업 등에 필요한 'AI-PET 융합형 기술' 개발이 중요

- 국내 산업에서 활용되는 다양한 프라이버시 기술이 글로벌 표준으로 연계하여 선도할 수 있도록 지원체계 마련 필요

  - 실 수요기반의 개인정보 보호·활용 관련 선도기술을 구현하고, 핵심기술은 국제 표준화를 추진하는 등 글로벌 역량 확보 추진

2 국내 개인정보 R&D 현황 분석

R&D 추진의 강점(Strength)

- 비식별·합성데이터 등 핵심 분야에서 세계 최고 수준의 정확도와 성능 확보
- 가명·익명처리 솔루션 등이 시범 운영 단계에 진입하여, 공공·금융·의료 등 산업현장에서 실증경험 축적
- 정부를 중심으로 '법·제도, 기술개발, 표준'이 연계된 정책-기술 통합 거버넌스를 구축
- 권위있는 논문지·국제학회 발표, 특허출원 등 산·학계 성과를 통해 개인정보 보호·활용 분야 글로벌 인지도 상승

R&D 추진의 약점(Weakness)

- 개인정보 분야 연구개발(R&D) 투자가 정보보안 대비 상대적으로 부족한 실정
- 에이전틱 AI, 로봇·물리 공간(피지컬 AI) 등 신기술 등장에 따른 프라이버시 위험에 대하여 대응 가능한 PET 개발 시급
- 국내에서는 서비스·플랫폼을 상용화하여 산업계로 확산하는 과정까지 선순환 체계가 초기단계로 안정적 생태계 조성이 필요
- 중소기업·스타트업 중심의 연구개발 구조로 인해 제품 마케팅, 국제 표준화 추진 등에 투입할 전문 인력·재원의 지속적 확보 어려움

R&D 추진의 기회(Opportunity)

- 생성형 AI 도입 확산과 신종 AI 기술 등장으로 인해 규율체계 준수 및 개인정보를 보호하기 위한 PET 도입 및 실증 수요 급증

  ※ (EU ENISA, 美 NIST, OECD 등) PET를 AI 협업 인프라 구축에 핵심 구성요소로 규정

- 개인정보 보호·활용 기술을 전용 인프라*를 통해 실증을 수행하여 국내 산업에 적합한 PET-AI 융합 모델을 연구개발 가능

  * '개인정보 이노베이션 존, 데이터 안심구역 등' 전용 인프라에서 실증 가능

R&D 추진의 위협(Threat)

- 신종 개인정보 활용 서비스*에 대응 가능한 연구개발이 미흡할 경우, 산업 현장에서는 서비스 이용에 따른 규율 사각지대 발생 우려

  * 에이전틱·피지컬 AI, 로봇, 메타버스, 자율주행 차량 등 실생활에 적용가능한 신기술

- 글로벌 빅테크 기업들의 적극적인 프라이버시 기술 개발로 인해 국내에서 개발한 기술이 후발·종속적 위치에 머무를 위험 상존

  ※ 연합학습, 차분프라이버시 등을 적용한 융합 PET 기술의 특허·표준 선점 필요

개인정보 전주기 보호 및 안전활용 기술 R&D 추진방향

① 정보주체의 권리를 보장하기 위한 권리행사·투명성·설명가능성 등 개인정보 보호·활용 기술을 선제적으로 개발

② AI·데이터 활용 시, 개인정보 생애주기 전 단계에서 유·노출 위험 등을 최소화하고 사후에도 적시 대응이 가능한 AI-PET 융합 기술로 고도화

③ 산업에서 안전하게 개인정보를 활용할 수 있는 상호운용 가능한 기술을 개발하고, 나아가 국제 표준으로 연계하는 등 세계 시장을 선점

SWOT 분석 결과

'AI 친화형·산업 연계·국제 표준 적합 PET 로드맵' 기반 기술개발 및 생태계 조성 필요

외부 환경 \ 내부 환경	Strength • 전 주기를 아우르는 개인정보 보호·활용 인프라 확보 • '정책→표준→R&D→실증'이 연계된 AI 친화형 거버넌스 구축	Weakness • 고난도 PET·AI 융합 분야에 대한 R&D 투자·인력·예산 규모 미흡 • 중·소·스타트업 중심 구조로 대형·국제 연계 R&D 수행 역량 제약
Opportunity • AI 친화형 PET 수요 급증 • 개인정보 이노베이션 존 등을 통한 국내·외 실증 및 협력 가능	① 기술개발 다각화 산업별 특성을 고려하여, 다양한 관점의 개인정보 보호·활용 기술 포트폴리오 구축 필요	③ 자원 집중화 난이도와 비용이 높은 분야는 거점형 연구센터·플래그십 과제로 모아 정부 차원의 집중투자 추진 필요
Threat • 글로벌 빅테크의 PET 기술·플랫폼 선점에 따른 기술 종속 위험 • 신기술 확산 속도 대비 규율 사각지대 발생 우려	② 최신기술 활용 기술개발 에이전틱·피지컬 AI 등 최신 기술을 활용하여, PET-AI 융합 엔진 등 연구 개발 필요	④ 기술개발 생태계 조성 산·학·연 공동 실증을 확대하고, 국제 챌린지·공동연구를 연계한 글로벌 협력 기반 R&D 생태계 조성 필요

개인정보 보호·활용 기술 발전 방향

개인정보 주권·권리 보장 | 개인정보 유·노출 위험 저감 | 개인정보 안전한 활용 지원 | AI 환경 선제적 대응 강화

3 개인정보 R&D 비전 및 추진방안

비 전

AI 시대, 국민이 안심할 수 있는 개인정보 전주기 보호·활용 선도국가

목 표 1
AI 시대에 대응하는
전주기 개인정보 보호·활용 기술 기반 구축

목 표 2
PET·AI 융합으로
안전한 데이터 활용과 개인정보 주권 보장

전 략	추 진 방 향
개인정보 주권 보장	• 동의·열람·정정·삭제·이동 등 권리 행사지원 기술 확보 • 디지털정부 환경에서 권리·통제권 가시화·자동화 기술 개발
유·노출 위험 경감	• 생애주기(설계(기획)-수집-이용-제공-파기) 전 단계 보호 기술 개발 • 다크웹·클라우드를 아우르는 탐지·차단·삭제증명 기술 개발
신뢰기반 안전활용	• 합성데이터·동형암호 등 PET 스택 고도화 기술 개발 • 의료·금융·공공 등 일상 분야별 안전활용 기술 개발
AI 대응 기술개발	• 에이전틱·피지컬 AI 전주기 프라이버시 안전성 평가 및 가드레일 기술 개발 • 연합학습·언러닝 등 AI-친화적 PET 내재화 기술 개발

기 대 효 과

Ⅳ 개념 및 기술분류

1. 개념 및 정의
2. 개인정보 보호·활용 기술과 정보보안 기술의 관계
3. 개인정보 전주기 보호·활용 기술 분류
   (Technology Tree)

CHAPTER Ⅳ

개념 및 기술분류

1 개념 및 정의

기본 개념

- '개인정보'란, 살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보로 정의
  - 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보와 가명정보를 포함

개인정보·가명정보·익명정보의 정의

「개인정보 보호법」 제2조

- [개인정보] 성명, 영상 등 해당 정보를 통해 개인을 알아볼 수 있거나 입수가능한 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 살아있는 개인에 관한 정보
- [가명정보] 개인정보를 추가정보 없이는 특정 개인을 알아볼 수 없게 가명처리*한 정보
  * 가명처리: 개인정보의 일부를 삭제하거나 일부 또는 전부 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리
- [익명정보] 시간, 비용, 기술을 고려했을 때 합리적으로 더 이상 개인을 알아볼 수 없는 정보로 개인정보가 아님

- '개인정보 보호'는 정보주체의 개인정보 자기결정권*을 철저히 보장하는 것을 의미
  * 자신에 관한 정보가 개인정보처리자로 부터 제3자에게 제공·이용하는 범위, 방법 및 시기 등을 정보주체가 스스로 결정할 수 있는 권리
  - 특히, 정보주체 권리보장을 위해 개인정보의 생애주기 특성에 맞는 보호와 안전한 활용을 위해서는 개인정보 보호·활용 기술이 필수적임

2 개인정보 보호·활용 기술과 정보보안 기술의 관계

개인정보 보호·활용을 위한 정보보안 기술의 한계

- 그간의 개인정보 보호는 법·제도를 중심으로 발전해왔으며, 기술적 보호는 정보보안 기술을 활용한 안전조치* 위주로 논의

  *「개인정보 보호법」 제29조(안전조치의무)에 따라 암호화, 접근통제 등 정보보안 기술 적용

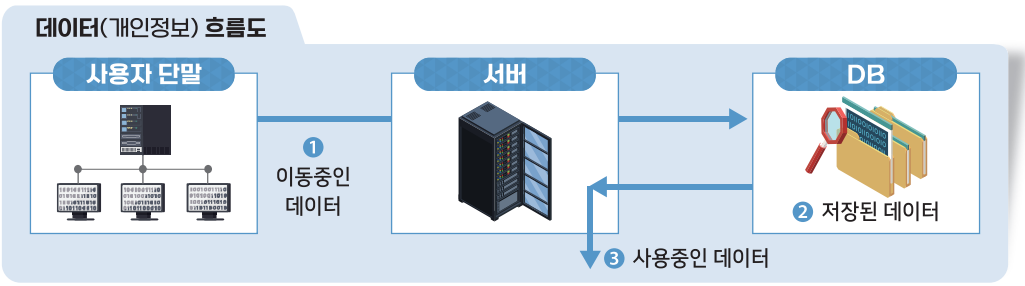
- 최근 빅데이터·인공지능 등 데이터 활용기술의 발전으로 데이터 활용 수요가 증가함에 따라 개인정보가 '안전 활용' 대상으로 인식 변화

- 개인정보의 처리 과정에서 노출 최소화, 오·남용 방지, 이용자 개인정보 보호 선호도 고려 등 프라이버시 보호에는 한계

  ※ 정보보안 기술은 인프라, 서비스 등의 기밀성·가용성·무결성 확보 기술 중심으로 발전

  - 특히, EU GDPR 등 정보주체 권리보장을 위해 강화되고 있는 각국의 개인정보 보호제도 준수 어려움

데이터 흐름 단계별 정보보안 기술 적용(예시)



❶ **개인정보 수집단계**: HTTPS, IPSec VPN 등 개인정보 암호화로 보호 가능
❷ **개인정보 저장단계**: DB 암호화, DB 접근통제 등으로 개인정보 보호 가능
❸ **개인정보 활용단계**: 개인정보 처리자 등에게 개인정보 노출 최소화를 위한 특화된 보호·활용 기술 필요

※ 암호화 데이터를 항시 복호화해야 하는 기존 정보보안 기술로는 한계

개인정보 보호·활용 기술과 정보보안 기술의 차별점

- 정보보안 기술은 시스템·데이터의 기밀성·무결성·가용성을 보장하기 위한 기술인 반면, 개인정보 보호·활용 기술은 그 목적이 광범위
  - 개인정보 보호·활용 기술은 개인정보 처리 과정에서 유출, 오·남용을 방지하고 정보주체의 자기결정권을 보장하기 위한 기술을 포함
  - 개인의 동의·선호 관리 등 정보주체의 권리를 보호하기 위한 기술은 정보보안 기술에 포함되지 않는 새로운 영역

- 국제 표준기구(ISO)에서는 정보보호 관리체계 표준*을 바탕으로 하여 개인정보보호 관리체계 표준**을 별도 제정('19.8.)
  - 개인정보 보호는 데이터의 생애주기를 반영한 관리 기준과 보호조치가 필요하다는 점을 반영

* ISO/IEC 27001 Information Security Management System

** ISO/IEC 27701 Privacy Information Management System

- 국내에서는 '18년 ISMS인증과 PIMS인증을 ISMS-P로 통합하면서, 정보보호 조치(ISMS)와 개인정보 보호 조치(+P)를 별도 구분

⇒ 개인정보의 보호와 안전한 활용을 지원하고 정보주체의 권리를 보장하기 위해 개인정보에 특화된 보호·활용 기술 필요

개인정보 보호·활용 기술과 정보보안 기술 비교

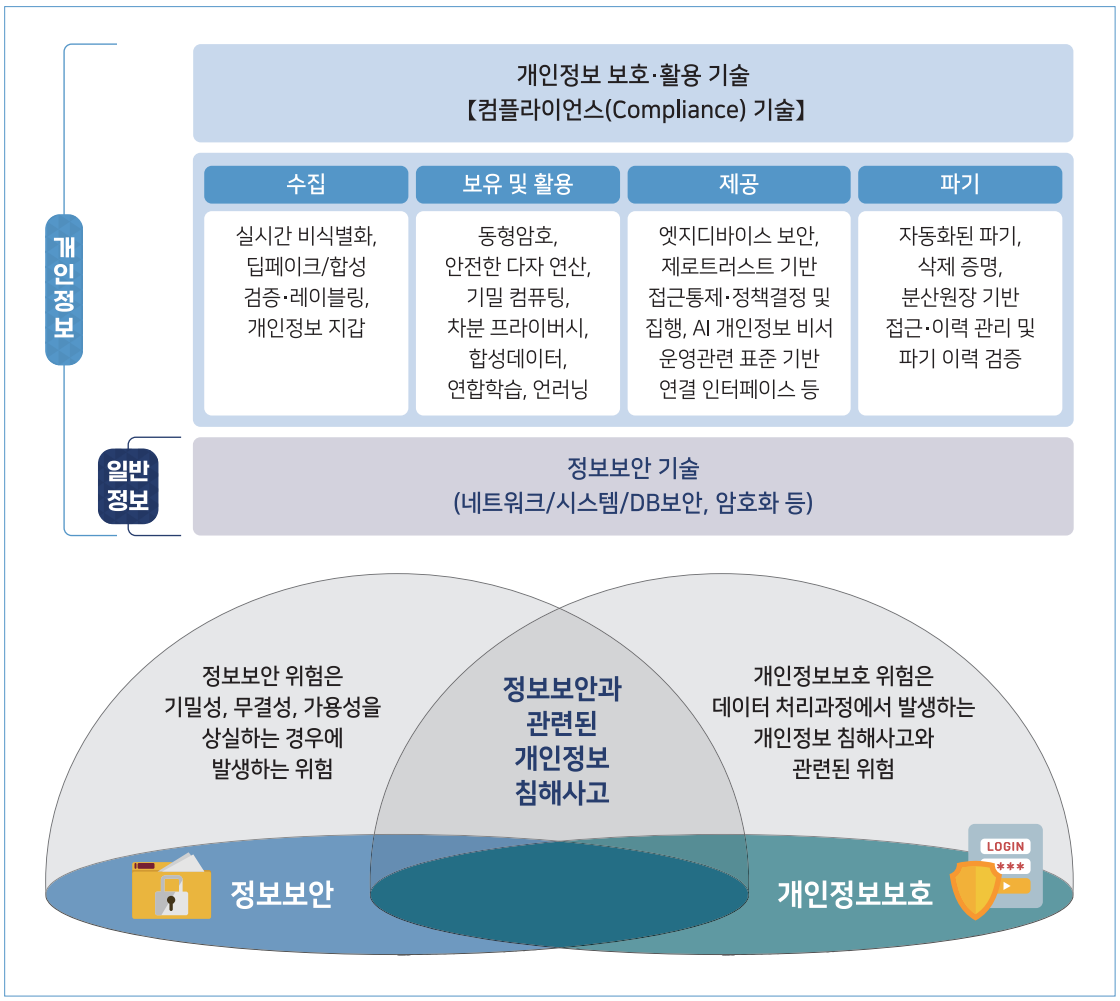
구 분	개인정보 보호·활용 기술	정보보안 기술
주요 보호대상	정보주체	ICT 인프라
보호 목적	정보주체의 권리 보장	기밀성, 무결성, 가용성 보장
기술개발 방향	개인정보의 보호와 안전한 활용 중심	시스템 보호 중심
프레임워크	수집-이용-저장-제공-파기	탐지-분석-대응-공유
정보주체 우선	O	X
주요 탐지대상	개인정보	일반 정보(시스템, 영업비밀 등)

개인정보 보호·활용 기술과 정보보안 기술의 관계

- 개인정보 보호·활용 기술은 정보보안 기술과 함께 발전해야 하는 상호 보완적 관계
  - 기업 등이 해킹사고가 발생하는 경우, 개인정보 유출 가능성이 높아 정보보안 기술은 개인정보를 보호하는 데 필수적 요소
  - 특히, 개인정보 생애주기 별 보호·활용 기술과 정보주체의 권리를 보호하는 기술이 적용되어야 완전한 개인정보 보호 가능

⇒ 정보보안 기술은 데이터 보호를 위한 1차 기반 기술이며, 최소한의 정보 처리, 유 노출 및 오 남용 방지 등 개인정보를 위한 2차 보호 기술 필요

개인정보 보호·활용 기술과 정보보안 기술 간 관계



3 개인정보 전주기 보호·활용 기술 분류 (Technology Tree)

개인정보 생애주기를 고려하여 4개의 축*을 중심으로 '개인정보 보호 및 안전한 활용 기술 분류체계'를 마련 ☞ 4개 중분류, 15개 소분류, 59개 세분류

① 개인정보 주권 보장	② 유·노출 위험 경감
③ 신뢰기반 안전활용	④ AI 대응 기술개발

- **(개정)** 국내·외 유관기관, 국제기구 등의 개인정보 기술 분류 및 활용체계를 분석하여, 국내의 정책·산업 환경 및 개인정보의 생애주기 흐름에 적합한 '전주기 보호·활용 기술 로드맵' 체계로 구성

  * 국제기구 별로 공개한 분류·가이드 참고 및 美 NIST, 美 NSTC, OECD, 국제표준 ISO/IEC 등의 관련 문서와 최신 기술연구 동향을 종합적으로 분석하여 도출

- **(의의)** AI 확산에 선제 대응하고, 개인정보 유출 위험을 경감하는 기술연구 등을 통해 변화된 환경에 능동적으로 대처할 수 있도록 기존의 분류체계를 보완·확장

분류체계의 목적과 범위

- 개인정보의 안전한 활용을 가능하게 하는 기술적 요소 전반을 포함

- 실제 산업현장에서 개인정보를 보호 및 활용에 필요한 핵심기술과 구성·운영 요소*를 하나의 기술 체계로 정리

  * (핵심기술) 차분 프라이버시, 동형암호 등 PET, (구성·운영 요소) 표준, 규격 등

기술 분류 시, 적용 및 제외 기준

- **(적용)** 개인정보 활용 과정에서 측정·검증·도입이 가능한 구성요소*

  * 개인정보 보호·활용에 필요한 '기술, 표준, 아키텍처, 프로세스, 기능, 응용 등'을 포함

- **(제외)** 기술을 실제로 구현·검증하는 대상이 아닌, 단순 문서작성 지원 또는 회의체 운영과 유사한 활동에 해당하는 요소

- **(검토)** ① 각 세분류 항목은 유형 1개만 부여 ② 동일 항목이 타 항목에서 필요한 경우 '대표-연계' 원칙 부여로 중복 가능성 제거

  ※ 예시: 기밀컴퓨팅 기술의 경우, 소분류 '3-1'을 대표 / '2-3'은 연계로 표기

체계 구조

- 본 기술 분류체계의 세분류는 다음 6가지 유형 중 하나로 정의하여 매칭(Matching)

① **(기술)** 구현 가능한 방법·엔진·모델
※ 차분 프라이버시, 안전한 다자 연산, 동형암호, 연합학습, 탐지 모델 등

② **(표준·규격)** 상호운용 및 검증을 위한 공식 스펙
※ 콘텐츠 출처 및 진위 보장을 위한 국제 협의체(C2PA), 자기주권신원(SSI)/탈중앙식별자(DID) 등

③ **(프레임워크·아키텍처)** 기술의 배치·조합·정책 이행 형태
※ 제로트러스트, 데이터 클린룸, 하이브리드 PET 등

④ **(평가·프로세스)** 검증·평가·스캐닝·정제 절차
※ 재식별 위험도 평가, 정적/동적 스캐닝 등

⑤ **(기능)** 사용자/운영 관점의 동작·기능
※ 정책 준수 증명 결과 열람, 경고/차단, 가드레일 등

⑥ **(응용·도메인)** 산업 분야별 구현 단위
※ 전자의무기록(EMR) PET 분석, 공공 통계, 메타버스 프라이버시 등

- 종전의 기술 R&D 및 표준화 로드맵*을 연속성 있도록 통합·연계하여 개정

* 개인정보 보호·활용 기술 R&D 로드맵('22~'26), 개인정보 보호·활용 기술 표준화 로드맵('23~'27)

(종전) 기술 R&D 로드맵	
중분류(3)	소분류(14)
1 정보주체 권리보장	1-1 정보주체 동의 실질화
	1-2 정보주체 통제권
	1-3 정보주체 신원인증 정보 관리
	1-4 개인정보 침해대응
2 유·노출 최소화	2-1 PbD 원칙을 적용한 기획·설계
	2-2 수집시 개인정보 탐지
	2-3 이용·제공시 개인정보 관리 강화
	2-4 개인정보 파기
	2-5 개인정보 안전성 확보
3 안전한 활용	3-1 안전활용 기반기술
	3-2 서비스 응용
	3-3 마이데이터 기반기술
	3-4 융합 프라이버시 보호
	3-5 인공지능 프라이버시

+

(종전) 표준화 로드맵	
중분류(3)	소분류(17)
1 정보주체 권리보장	1-1 정보주체 권리보장 체계
	1-2 정보주체 동의
	1-3 정보주체 통제권
	1-4 정보주체 신원인증 정보관리
	1-5 개인정보 침해대응
2 처리단계별 보호 강화	2-1 개인정보 처리단계 체계
	2-2 PbD 원칙을 적용한 기획·설계
	2-3 수집
	2-4 이용·제공
	2-5 파기
	2-6 안전성확보
3 안전한 활용	3-1 안전한 활용 체계
	3-2 기반기술
	3-3 서비스 응용
	3-4 마이데이터 개인정보 보호
	3-5 융합 프라이버시 보호
	3-6 인공지능 서비스 프라이버시 보호

⬇

(개정) 기술 R&D 및 표준화 로드맵		
중분류(4)	소분류(15)	세분류(59)
1 개인정보 주권 보장	1-1 정보주체 동의의 실질화	동적 동의 관리
	1-2 정보주체 통제권	정책 준수 증명 결과 열람
	1-3 정보주체 신원인증 정보 관리	개인정보 지갑
2 유·노출 위험 경감	2-1 수집 시 개인정보 탐지	실시간 비식별화(엣지/온디바이스 등) 등 2개
	2-2 개인정보 파기	자동화된 파기 등 2개
	2-3 개인정보 안전성 확보	플랫폼 무결성/신뢰실행환경(TEE) 등 7개
	2-4 외부 유출 모니터링·탐지	다크웹·표면웹 유출 탐지 등 4개
3 신뢰기반 안전활용	3-1 안전활용 기반기술	데이터 정제·전처리, 비식별/변환 등 11개
	3-2 서비스 응용	합성 임상데이터, 합성 통계데이터 등 7개
	3-3 마이데이터 기반 기술	데이터 클린룸·데이터 스페이스 연계 PET 등 3개
4 AI 대응 기술개발	4-1 AI 모델 학습단계 프라이버시	언러닝(Unlearning) 등 4개
	4-2 AI 모델 프라이버시 공격·방어 및 안전성 평가	AI 모델 안전성 평가 등 5개
	4-3 AI 콘텐츠 신뢰성·출처	생성·합성콘텐츠 탐지·표시 등 2개
	4-4 AI 에이전트 보안	에이전트·도구·로봇 실행 보안 등 3개
	4-5 AI 기반 개인정보 탐지·비식별화	피지컬 AI/로봇 센싱 프라이버시 등 6개

- 세분류 별로 개인정보 수집부터 파기까지 생애주기와 연계하여 정의
  - '기술'을 중심으로 '구현·검증·운영 등' 개인정보 처리 전 절차에 영향을 미치는 요소를 도출하여 **분류체계(중분류4-소분류15-세분류59)** 구성

개인정보 보호·활용 기술 분류체계

중분류(4)	소분류(15)	세분류(59)	개인정보 생애주기				비고
			수집·저장	처리·학습	공유·활용	파기·사후	
1 개인정보 주권 보장	1-1 정보주체 동의의 실질화	① 동적 동의 관리	●	●	●		대표 (3-3 연계)
	1-2 정보주체 통제권	① 정책 준수 증명 결과 열람		●	●		
	1-3 정보주체 신원인증 정보 관리	① 개인정보 지갑 (자기주권신원(SSI)/탈중앙식별자 (DID, Decentralized Identifier))	●	●	●		
2 유·노출 위험 경감	2-1 수집 시 개인정보 탐지	① 실시간 비식별화(엣지/온디바이스 등)	●				
		② 딥페이크/합성 검증·레이블링	●				
	2-2 개인정보 파기	① 자동화된 파기				●	
		② 삭제 증명(Proof of Erasure)				●	
	2-3 개인정보 안전성 확보	① 양자내성 암호화	●	●	●		
		② 플랫폼 무결성/신뢰실행환경(TEE)	●	●	●		연계 (3-1⑪ 대표)
		③ 분산원장 기반 접근제어	●	●	●		
		④ 엣지 디바이스 개인정보보호	●	●	●		
		⑤ 하이브리드 PET(동형암호+신뢰 실행 환경 등)	●	●	●		대표 (3-1⑧ 연계) 연계 (3-1⑪ 대표)
		⑥ PET 엔진(GPU/NPU) 가속·경량화(가속 커널/컴파일러/오프로딩 등)	●	●	●		
		⑦ 제로트러스트 기반 접근통제·정책결정/집행	●	●	●		
	2-4 외부 유출 모니터링·탐지	① 다크웹·표면웹 유출 탐지		●	●	●	
		② 공개저장소·클라우드 노출 스캐닝		●	●	●	
		③ 공개출처정보(OSINT) 정규화		●	●	●	
		④ 문서·이미지 콘텐츠 지문(퍼셉추얼 해시)		●	●	●	

중분류(4)	소분류(15)	세분류(59)		개인정보 생애주기				비고
				수집·저장	처리·학습	공유·활용	파기·사후	
3 신뢰기반 안전활용	3-1 안전활용 기반기술	데이터 정제·전처리	① 개인정보 제거·마스킹	●	●	●		
			② 라이선스 검증·출처추적	●	●	●	●	
			③ 중복/오염 제거	●	●	●		
			④ 정적·동적 스캐닝 (코드·문서·데이터)	●	●	●	●	
		비식별/변환	⑤ 정형데이터 비식별화	●	●	●		
			⑥ 비정형데이터 비식별화 (영상, 텍스트, 음성 등)	●	●	●		
			⑦ 재식별 위험도 평가·검증		●	●	●	
			⑧ 합성데이터 등 PET 기반 비식별화(단일·하이브리드)	●	●	●		연계 (2-3⑤ 대표)
		프라이버시 보존 연산	⑨ 동형암호(HE)	●	●	●		
			⑩ 안전한 다자 연산(SMPC)	●	●	●		
			⑪ 기밀컴퓨팅(신뢰실행환경·기밀컴퓨팅 가상머신·원격증명)	●	●	●		대표 (2-3⑤ 연계)
	3-2 서비스 응용	① (의료·공공) 합성 임상데이터, 합성 통계데이터 등			●	●		
		② (금융) 동형암호(HE)/안전한 다자 연산(SMPC) 기반 자금세탁방지(AML)·고객신원확인(KYC) 분석			●	●		
		③ (금융) 프라이버시 보호 신용평가 등			●	●		
		④ (의료) 전자의무기록(EMR) 등의 PET 분석			●	●		
		⑤ (공공) 차분 프라이버시를 적용하여 개인정보 위험을 낮춘 데이터 공개			●	●		차분 프라이버시 계열 (4-1① 연계)
		⑥ (일반) 생활속에서의 프라이버시 영상 보호(CCTV, 현관문 카메라 등)		●	●	●		
		⑦ 기타 메타버스 환경 등에서의 프라이버시 보호			●	●		
	3-3 마이데이터 기반기술	① 데이터 클린룸·데이터스페이스 연계 PET			●	●		대표 (3-1~2 연계)
		② 마이데이터 동의·위임 통합 자동화 플랫폼		●	●	●	●	연계 (1-1~3 대표)
		③ 마이데이터-AI 개인정보 비서 연동·운영		●	●	●	●	연계 (4-4~5 대표)

중분류(4)	소분류(15)	세분류(59)	개인정보 생애주기				비고
			수집·저장	처리·학습	공유·활용	파기·사후	
4 AI 대응 기술개발	4-1 AI 모델 학습단계 프라이버시	① 차분 프라이버시(DP) 적용(LLM 파인튜닝·학습 프레임워크)		●			차분 프라이버시 계열 (3-2⑤ 연계)
		② 언러닝(Unlearning)		●		●	
		③ 연합학습(FL, Federated Learning)		●			
		④ 합성데이터 생성·정제·검증(학습용)	●	●			합성데이터 계열(3-1⑧, 3-2①, 4-2⑤ 연계)
	4-2 AI 모델 프라이버시 공격·방어 및 안전성 평가	① 정렬 파인튜닝 (인간 피드백 기반 강화학습(RLHF)/ 선호신호 직접 최적화(DPO)/ 그룹 비교 정렬 최적화(GRPO))		●			
		② AI 모델 안전성 평가		●	●		
		③ 설명가능/감사가능 AI(XAI/Auditable AI)		●	●	●	
		④ 실시간(데이터 스트림) 입·출력 가드레일		●	●		
		⑤ 합성데이터 기반 학습·증강(분포 정합/ 혼합비율 최적화)	●	●			합성데이터 계열(3-1⑧, 3-2①, 4-1④ 연계)
	4-3 AI 콘텐츠 신뢰성·출처	① 콘텐츠 출처 및 진위 보장을 위한 국제 협의체(C2PA)/워터마킹 등 출처·이력 설계		●	●		
		② 생성·합성콘텐츠 탐지·표시(실시간 경고·차단 포함)		●	●		
	4-4 AI 에이전트 보안	① 에이전트·도구·로봇 실행 보안	●	●	●	●	대표 (3-3 연계)
		② AI 개인정보 비서 운영 관련 표준 기반 연결 인터페이스(모델 컨텍스트 프로토콜(MCP))	●	●	●	●	
		③ 피지컬 AI 실시간 프라이버시 제어	●	●	●	●	
	4-5 AI 기반 개인정보 탐지·비식별화	① 코드 시크릿 탐지 엔진	●	●	●	●	
		② 문서·이미지·음성 개인정보 탐지	●	●	●	●	
		③ 멀티모달 개인정보 검출(비전-언어모델 (VLM) 기반 크로스 모달)	●	●	●	●	
		④ AI기반 정형데이터 비식별화	●	●	●	●	
		⑤ AI기반 비정형데이터 비식별화(영상, 텍스트, 음성 등)	●	●	●	●	
		⑥ 피지컬 AI/로봇 센싱 프라이버시	●	●	●	●	

분류체계 내 소분류 및 세분류 정의

소분류 및 세분류	개념
1-1 정보주체 동의의 실질화	정보주체가 자신의 개인정보 처리 목적·범위를 이해하고 동의 여부를 능동적으로 관리할 수 있도록 동의 절차를 설계·운영하는 기술
① 동적 동의 관리	서비스 이용 맥락과 위험 수준에 따라 동의 범위와 옵션을 실시간으로 조정·갱신하고, 정보주체가 언제든 변경·철회할 수 있게 지원하는 기술
1-2 정보주체 통제권	정보주체가 자신의 개인정보 이용 현황과 권리 행사 결과를 쉽게 확인하고 통제할 수 있도록 투명성을 제공하는 기술
① 정책 준수 증명 결과 열람	개인정보 처리자가 법·정책·내부 규정을 얼마나 준수했는지에 대한 증명 결과를 정보주체가 온라인으로 열람·검증할 수 있게 하는 기술
1-3 정보주체 신원인증 정보 관리	정보주체의 신원인증 정보와 자격 증명을 안전하게 저장·관리하고 필요 시 최소한으로 제시할 수 있게 지원하는 기술
① 개인정보 지갑(자기주권신원(SSI))/탈중앙식별자(DID))	개인정보 지갑 자기주권신원 탈중앙식별자를 이용해 사용자가 자신의 신원·자격 정보를 스스로 보관·제어하고, 필요한 서비스에 선택적으로 제공할 수 있게 하는 기술
2-1 수집 시 개인정보 탐지	개인정보가 수집되는 시점에 민감정보 포함 여부를 자동으로 탐지하고 위험을 줄이도록 지원하는 기술
① 실시간 비식별화 (엣지/온디바이스 등)	엣지·온디바이스 환경에서 개인정보를 서버로 보내기 전에 실시간으로 식별 요소를 삭제·대체하여 노출을 최소화하는 기술
② 딥페이크/합성 검증·레이블링	영상·음성·이미지 등에서 딥페이크·합성 콘텐츠 여부를 판별하고, 개인정보가 포함된 부분을 식별·레이블링하는 기술
2-2 개인정보 파기	불필요해진 개인정보를 지체 없이 안전하게 파기하고, 파기 여부를 검증·증명할 수 있도록 지원하는 기술
① 자동화된 파기	보유 기간·목적 달성 여부 등에 따라 개인정보를 자동으로 탐지하고 물리적·논리적으로 안전하게 삭제하는 기술
② 삭제 증명(Proof of Erasure)	삭제 수행 내역을 암호학적으로 기록·검증하여 개인정보가 더 이상 복구 불가능한 상태로 파기되었음을 증명하는 기술
2-3 개인정보 안전성 확보	저장·전송·처리 과정 전반에서 개인정보를 외부 공격과 내부 오남용으로부터 안전하게 보호하기 위한 기반 보안 기술
① 양자내성 암호화	양자컴퓨터 시대에도 안전하도록 설계된 암호 알고리즘을 활용해 개인정보를 장기적으로 보호하는 기술
② 플랫폼 무결성/신뢰실행환경(TEE)	플랫폼·단말의 부팅부터 실행까지 위변조 여부를 검증하고, 신뢰실행환경을 통해 민감 연산과 데이터를 격리·보호하는 기술

소분류 및 세분류	개념
③ 분산원장 기반 접근제어	블록체인 등 분산원장을 활용하여 접근 권한과 이력을 투명하게 기록하고 위변조를 방지하는 접근제어 기술
④ 엣지 디바이스 개인정보보호	IoT·모바일 등 엣지 단말의 인증·펌웨어·통신을 강화해 현장에서 수집되는 개인정보를 안전하게 보호하는 기술
⑤ 하이브리드 PET (동형암호+신뢰실행환경 등)	동형암호·신뢰실행환경 등 서로 다른 프라이버시 보호 기법을 결합해 보안성과 성능을 동시에 확보하는 융합 환경의 보호 기술
⑥ PET 엔진(GPU/NPU) 가속·경량화 (가속커널/컴파일러/연산분담 등)	GPU·NPU 등 전용 하드웨어를 활용해 PET 알고리즘을 고속·경량으로 실행하기 위한 가속 커널·컴파일·연산분담 기술
⑦ 제로 트러스트 기반 접근통제 정책결정 및 집행	사용자·기기·네트워크를 항상 검증하는 제로 트러스트 원칙에 따라 접근통제·정책결정·집행을 통합적으로 수행하는 기술
2-4 외부 유출 모니터링·탐지	다크웹·오픈웹 등 외부 공간으로 유출된 개인정보 징후를 지속적으로 탐색·모니터링하는 기술
① 다크웹·표면웹 유출 탐지	다크웹·표면웹의 게시글·거래 정보를 수집·분석하여, 특정 기관·개인의 개인정보 유출 정황을 탐지하는 기술
② 공개저장소·클라우드 노출 스캐닝	GitHub·클라우드 스토리지 등 공개된 저장소와 클라우드 환경을 주기적으로 점검해 비인가 개인정보 노출을 탐지하는 기술
③ 공개출처정보(OSINT) 정규화	뉴스·SNS·포럼 등 다양한 공개출처정보를 수집·정규화하여 개인정보 유출 징후를 분석·판단에 활용하는 기술
④ 문서·이미지 콘텐츠 지문(퍼셉추얼 해시)	문서·이미지에 대해 내용 기반으로 디지털 지문인 퍼셉추얼 해시를 생성·비교하여 동일·유사한 개인정보 콘텐츠의 확산 여부를 추적하는 기술
3-1 안전활용 기반기술	데이터의 품질을 개선하고 안전한 비식별·변환·연산을 위한 기초 처리를 수행해 개인정보의 안전한 활용을 뒷받침하는 기술
ㅣ 데이터 정제·전처리	분석·학습 전에 데이터에서 오류·노이즈·불필요한 개인정보를 정리해 활용 가능성과 안전성을 높이는 기술
① 개인정보 제거·마스킹	데이터셋에서 성명·연락처 등 개인식별정보를 삭제하거나 대체값으로 변환하여 노출을 최소화하는 기술
② 라이선스 검증·출처추적	데이터의 수집 근거·이용 동의·저작권·출처를 확인·기록해 적법한 활용을 보장하는 기술
③ 중복/오염 제거	중복 레코드·비정상 값·악성 삽입 데이터 등을 자동 탐지·정제해 데이터 품질을 높이는 기술
④ 정적·동적 스캐닝 (코드·문서·데이터)	코드·문서·데이터를 정적·실행 시점에서 분석해 숨겨진 개인정보·취약점·민감정보 패턴을 찾아내는 기술

소분류 및 세분류	개념
2 비식별/변환	개인·집단을 직접 식별할 수 없도록 데이터를 변환하면서 분석·통계 활용 유용성을 유지하는 기술
⑤ 정형데이터 비식별화	표 형태의 정형데이터에서 식별자를 삭제·범주화·총계처리 등으로 재식별 위험을 낮추는 기술
⑥ 비정형데이터 비식별화 (영상, 텍스트, 음성 등)	영상·텍스트·음성 등 비정형데이터에서 얼굴·음성·이름 등 식별 요소를 자동 탐지·가림 처리하는 기술
⑦ 재식별 위험도 평가·검증	비식별 처리 후에도 특정 개인이 다시 식별될 가능성을 정량적으로 평가·검증하는 기술
⑧ 합성데이터 등 PET 기반 비식별화 (단일·하이브리드)	합성데이터·동형암호·차분프라이버시(집계형)·연합학습 등 다양한 PET를 상황에 맞게 단일 혹은 조합하여 보호 목적에 맞게 비식별화된 데이터로 변환하는 기술
3 프라이버시 보존 연산	암호화·분산연산·기밀컴퓨팅 등을 활용해 원본을 노출하지 않고 데이터 간 연산·분석을 수행하는 기술
⑨ 동형암호(HE)	암호문 상태에서 통계·모델 연산을 수행하고 결과만 복호화하여 확인하는 방식으로 개인정보를 보호하는 기술
⑩ 안전한 다자 연산(SMPC)	여러 참여자가 서로의 원본 데이터를 공개하지 않고 합계·교집합 등 공동 연산 결과만 공유하는 기술
⑪ 기밀컴퓨팅(신뢰실행환경·기밀컴퓨팅 가상머신·원격증명)	신뢰실행환경·기밀 컴퓨팅 가상머신·원격증명 등을 활용해 클라우드·공유환경에서도 개인정보 관련 연산·데이터를 하드웨어 수준으로 격리하는 기술
3-2 서비스 응용	의료·금융·공공·생활서비스 등 각 분야에서 프라이버시 강화 기술을 적용해 실제 서비스와 비즈니스에 개인정보 보호를 내재화하는 기술
① (의료·공공) 합성 임상데이터, 합성 통계데이터 등	실제 환자·국민 정보를 대체하는 합성 임상·통계데이터를 생성·관리해 연구·정책 분석에 안전하게 활용하는 기술 등을 가리킴
② (금융) 동형암호(HE)/다자간 연산(MPC) 기반 자금세탁방지(AML)·고객신원확인(KYC) 분석	동형암호·다자간 연산을 활용해 원본 계좌·신원 정보를 노출하지 않고 자금세탁방지(AML)나 혹은 고객신원확인(KYC) 위험 분석을 수행하는 기술
③ (금융) 프라이버시 보호 신용평가 등	소득·소비 패턴을 프라이버시 보호 방식으로 분석해 차별과 과도한 노출 없이 신용도를 평가하는 기술 등을 가리킴
④ (의료) 전자의무기록(EMR) 등 PET 분석	전자의무기록 등에 프라이버시 강화 기술을 적용해 진료·연구·통계를 지원하면서 환자 개인정보를 보호하는 기술
⑤ (공공) 차분 프라이버시(DP) 등 기반 공공데이터 공개	차분 프라이버시 등을 적용하여 공공 통계·지표를 공개하면서도 개별 국민의 정보를 유추 등 식별할 수 없게 하는 기술
⑥ (일반) 생활속에서의 프라이버시 영상 보호(CCTV, 현관문 카메라 등)	CCTV·초인종 카메라 등 생활 영상에서 얼굴·차량번호 등 개인정보를 자동 식별·가림 처리해 프라이버시를 보호하는 기술
⑦ 기타 메타버스 환경 등에서의 프라이버시 보호	기타 메타버스·가상공간 등에서 위치·음성·아바타 정보 등을 과도하게 추적·결합하지 않도록 설계·제어하는 프라이버시 보호 기술

소분류 및 세분류	개념
3-3 마이데이터 기반기술	마이데이터 생태계에서 개인이 자신의 데이터 이동·결합·활용을 안전하게 관리할 수 있도록 하는 기반 기술
① 데이터 클린룸·데이터스페이스 연계 PET	마이데이터로 이동·위임된 개인데이터를 데이터 클린룸·데이터스페이스에서 원본 노출 없이 결합·분석하기 위한 PET 연계 기술
② 마이데이터 동의·위임 통합 자동화 플랫폼	여러 기관·서비스에 분산된 동의·위임·열람·정정 요청을 마이데이터 허브·플랫폼에서 통합 관리하고 표준 API로 연동하는 인프라 기술
③ 마이데이터-AI 개인정보 비서 연동·운영	AI 개인정보 비서가 마이데이터 허브·데이터스페이스와 안전하게 연결되어, 동의 관리·열람·정정·삭제 요청을 자동 수행하도록 지원하는 연동 서비스 및 게이트웨이 기술
4-1 AI 모델 학습단계 프라이버시	AI 모델 학습 단계에서부터 개인정보 유출·편향을 줄이기 위해 데이터·모델을 설계·관리하는 기술
① 차분 프라이버시(DP) 적용(LLM 파인튜닝·학습 프레임워크)	대규모 언어모델 학습·파인튜닝 과정에 차분 프라이버시를 적용해 개별 학습 샘플이 노출되지 않도록 노이즈를 관리하는 기술
② 언러닝(Unlearning)	학습된 모델에서 특정 데이터의 영향을 선택적으로 제거해 삭제 요구나 과도한 학습을 반영할 수 있도록 하는 기술
③ 연합학습(FL)	여러 기관·단말이 데이터를 공유하지 않고 연합학습으로 공동 모델을 학습해 개인정보 노출을 줄이는 기술
④ 합성데이터 생성·정제·검증(학습용)	AI 학습용 합성데이터를 생성·정제·검증해 원본 데이터 의존도를 낮추면서도 모델 자체의 성능을 유지하는 기술
4-2 AI 모델 프라이버시 공격·방어 및 안전성 평가	AI 모델에 대한 프라이버시 공격·오용 위험을 평가·완화하고, 안전한 응답을 보장하기 위한 정렬·평가·방어 기술
① 정렬 파인튜닝(인간 피드백 기반 강화학습(RLHF)/ 선호신호 직접 최적화(DPO)/ 그룹 비교 정렬 최적화(GRPO))	인간 피드백 기반 강화학습(RLHF)/선호신호 최적화(DPO)/그룹 비교 정렬 최적화(GRPO) 등을 활용하여 인간 선호와 규범에 맞게 AI 모델의 응답을 조정·정렬하는 기술
② AI 모델 안전성 평가	프롬프트 공격·훈련데이터 누설 등 위험 시나리오를 정의하고 표준화된 테스트 데이터셋을 이용하여 모델의 안전성을 체계적으로 측정하는 기술
③ 설명가능/감사가능 AI (XAI/Auditable AI)	AI 의사결정 과정을 설명 가능하게 만들고 외부 감사·검증이 가능하도록 로그와 근거를 제공하는 기술
④ 실시간(데이터 스트림) 입·출력 가드레일	스트리밍 환경에서 입력·출력을 실시간 모니터링하고 위험 콘텐츠를 차단·완화하는 AI 가드레일 기술
⑤ 합성데이터 기반 학습·증강(분포 정합/혼합비율 최적화)	합성데이터를 활용해 모델 학습·증강 시 데이터 분포와 혼합비율을 조정해 편향·프라이버시 위험을 줄이는 기술

소분류 및 세분류	개념
4-3 AI 콘텐츠 신뢰성·	생성·합성된 AI 콘텐츠의 출처와 진위를 검증하고 위조·오남용을 막기 위한 신뢰 기반 기술
① 콘텐츠 출처 및 진위 보장을 위한 국제 협의체(C2PA)/워터마킹 등 출처·이력 설계	C2PA의 공개된 기술규격 표준사양, 워터마킹 기술 등을 활용하여 콘텐츠 생성·편집 이력을 기록하고 출처를 검증 가능하게 하는 기술
② 생성 합성콘텐츠 탐지·표시(실시간 경고·차단 포함)	딥페이크·합성 이미지·텍스트를 자동 탐지하고 사용자에게 명확히 표시하거나 실시간 경고·차단하는 기술
4-4 AI 에이전트 보안	에이전트형 AI·로봇이 다양한 도구·센서와 연동되는 환경에서 프라이버시 침해와 오작동을 방지하는 기술
① 에이전트·도구·로봇 실행 보안	에이전트·도구·로봇 실행 흐름을 검증·모니터링해 비인가 명령·위험 행동을 차단하는 실행 보안 기술
② AI 개인정보 비서 운영 관련 표준 기반 연동 인터페이스(모델 컨텍스트 프로토콜(MCP))	모델 컨텍스트 프로토콜 등 표준 인터페이스를 활용해 AI 개인정보 비서가 여러 시스템·데이터에 안전하게 연결·동작하도록 관리하는 기술
③ 피지컬 AI 실시간 프라이버시 제어	카메라·센서를 포함하는 피지컬 AI·로봇의 위치·영상·음성 수집 범위를 제어해 산업 현장에서 프라이버시를 보호하는 기술
4-5 AI 기반 개인정보 탐지·비식별화	코드·문서·영상·센싱데이터 등 다양한 형태의 정보에서 개인정보를 자동 탐지·비식별화하는 AI 기반 기술
① 코드 시크릿 탐지 엔진	소스코드·설정파일 등에서 API 키·비밀번호 등 시크릿 정보를 자동 탐지·경고하는 기술
② 문서·이미지 음성 개인정보 탐지	문서·이미지·음성에서 이름·주소·음성 특징 등 민감 정보를 인식·추출해 표시하거나 가리기 위한 기술
③ 멀티모달 개인정보 검출(비전-언어모델(VLM) 기반 크로스 모달)	비전-언어 모델(VLM)이 텍스트·이미지·음성 사이를 오가며 이해하고, 텍스트↔이미지↔음성에 흩어진 개인정보를 서로 연결·대조해 찾아내는 기술
④ AI기반 정형데이터 비식별화	AI 모델을 활용해 정형데이터의 비식별 처리 방식을 자동 추천·적용하고 품질을 평가하는 기술
⑤ AI기반 비정형데이터 비식별화 (영상, 텍스트, 음성 등)	AI를 이용해 영상·텍스트·음성 등 비정형데이터의 개인정보 영역을 정밀하게 탐지·마스킹 처리하는 기술
⑥ 피지컬 AI/로봇 센싱 프라이버시	카메라·라이다 등 로봇 센서가 수집하는 주변 인간·환경 정보를 필요 최소한으로 활용이 가능하도록 프라이버시를 제어하는 기술

V 대상 기술 선정

1. R&D 추진을 위한 핵심기술 선정
2. 최종 선정된 로드맵 대상 핵심기술 및 표준

CHAPTER V

대상 기술 선정

1 R&D 추진을 위한 후보 기술 선정

개인정보 분야의 산·학·연 전문가로 구성된 「개인정보 R&D 중장기 로드맵 개정 연구」 결과, 11개 핵심기술 도출

- 다음의 검토기준에 따라 중요도를 상대 평가하고, 개발 필요성이 높은 순으로 로드맵 대상 기술 11개 선정

로드맵 대상 기술 검토 기준

❶ 정부 R&D 지원 필요성이 있는 기술(민간 영역은 제외)
❷ 위험도, 혁신성 및 기존 지원 여부를 고려하여 고위험·도전적 기술
❸ 국민 생활문제와 국민 삶의 질 향상에 필요한 사회문제 해결형 R&D 기술
❹ R&D 추진 시급성 또는 국산화 필요성이 높은 기술

[범례] ⦿ 매우 높음 / ● 높음 / ○ 보통 / - 낮음

※ 기준 ❶~❹ 표시는 전문가 의견조사 결과를 바탕으로 각 기술이 정의한 검토기준에 따른 부합성 정도 및 상대적 합의 강도를 표식화 함(⦿ 매우 높음, ● 높음, ○ 보통)

※ 종합판정은 59개 전체 기술의 절대적 중요도나 필요성의 유무를 의미하는 것이 아니며, 본 로드맵에서의 중점 검토 및 단계적 추진 필요성을 기준으로 한 상대적 분류 결과임

※ 핵심기술(11개)은 종합판정 결과와 함께 정책 연계성, 기술 파급효과, 기술 간 중복성 및 통합 가능성 등을 종합적으로 고려하여 최종 선정하였으며, 상대적으로 중요도가 높은 차순위 후보기술(7개)도 평가 병행

- 주요 분야 별 핵심기술 ※ 핵심기술 11개
  - 정보주체가 인식하지 못하는 개인정보 수집을 방지하는 등 정보주체의 자기정보 통제권을 보장하기 위한 기술 ☞ **1개**
  - 개인정보 침해사고를 예방하고 현행 규율·관리 체계의 사각지대를 보완하는 기술 ☞ **3개**
  - 개인정보의 안전한 활용을 위한 재식별 위험도 평가·검증 등 기술 ☞ **3개**
  - 에이전틱·피지컬 AI 등 최근 등장하고 있는 각종 AI 환경에서 개인정보 보호를 위한 대응 기술 ☞ **4개**

개인정보 보호·활용 기술 분류체계(59개) 대상, 핵심기술 선정 결과

중분류(4)	소분류(15)	세분류(59)	기준 ❶	기준 ❷	기준 ❸	기준 ❹	종합 판정	선정 단계
❶ 개인정보 주권 보장	❶-1 정보주체 동의의 실질화	① 동적 동의 관리	●	○	●	○	하	기타 검토기술
	❶-2 정보주체 통제권	**① 정책 준수 증명 결과 열람**	⦿	⦿	⦿	⦿	**상**	**핵심기술**
	❶-3 정보주체 신원인증 정보 관리	① 개인정보 지갑(자기주권신원(SSI)/탈중앙식별자(DID, Decentralized Identifier))	●	○	●	⦿	중	후보기술
❷ 유·노출 위험 경감	❷-1 수집 시 개인정보 탐지	① 실시간 비식별화 (엣지/온디바이스 등)	⦿	●	●	○	중	후보기술
		② 딥페이크/합성 검증·레이블링	⦿	⦿	⦿	⦿	**상**	**핵심기술**
	❷-2 개인정보 파기	① 자동화된 파기	●	○	⦿	●	중	후보기술
		② 삭제 증명(Proof of Erasure)	●	○	○	●	하	기타 검토기술
	❷-3 개인정보 안전성 확보	① 양자내성 암호화	●	●	○	●	하	기타 검토기술
		② 플랫폼 무결성/신뢰실행환경 (TEE)	●	●	○	●	하	기타 검토기술
		③ 분산원장 기반 접근제어	○	●	○	○	하	기타 검토기술
		④ 엣지 디바이스 개인정보보호	⦿	⦿	⦿	⦿	**상**	**핵심기술**
		⑤ 하이브리드 PET(동형암호+신뢰실행 환경 등)	●	●	○	●	하	기타 검토기술
		⑥ PET 엔진(GPU/NPU) 가속·경량화(가속 커널/컴파일러/오프로딩 등)	○	●	○	●	하	기타 검토기술
		⑦ 제로트러스트기반 접근통제 정책결정/집행	●	●	○	●	하	기타 검토기술
	❷-4 외부 유출 모니터링·탐지	**① 다크웹·표면웹 유출 탐지**	⦿	⦿	⦿	⦿	**상**	**핵심기술**
		② 공개저장소·클라우드 노출 스캐닝	●	●	○	●	하	기타 검토기술
		③ 공개출처정보(OSINT) 정규화	○	●	○	○	하	기타 검토기술
		④ 문서·이미지 콘텐츠 지문 (퍼셉추얼 해시)	○	●	○	○	하	기타 검토기술

중분류(4)	소분류(15)	세분류(59)		기준 ❶	기준 ❷	기준 ❸	기준 ❹	종합 판정	선정 단계
3 신뢰기반 안전활용	3-1 안전활용 기반기술	데이터 정제·전처리	① 개인정보 제거·마스킹	●	○	●	○	하	기타 검토기술
			② 라이선스 검증·출처추적	○	○	●	○	하	기타 검토기술
			③ 중복/오염 제거	○	○	●	○	하	기타 검토기술
			④ 정적·동적 스캐닝 (코드 문서 데이터)	●	●	○	●	하	기타 검토기술
		비식별/변환	⑤ 정형데이터 비식별화	●	○	●	○	하	기타 검토기술
			⑥ 비정형데이터 비식별화 (영상, 텍스트, 음성 등)	●	●	○	●	하	기타 검토기술
			⑦ 재식별 위험도 평가·검증	⊙	⊙	⊙	⊙	**상**	**핵심기술**
			⑧ 합성데이터 등 PET 기반 비식별화 (단일·하이브리드)	⊙	⊙	⊙	⊙	**상**	**핵심기술**
		프라이버시 보존 연산	⑨ 동형암호(HE)	●	●	○	●	하	기타 검토기술
			⑩ 안전한 다자 연산 (SMPC)	●	●	○	●	하	기타 검토기술
			⑪ 기밀컴퓨팅(신뢰 실행환경·기밀컴퓨팅 ·가상머신·원격증명)	●	●	○	●	하	기타 검토기술
	3-2 서비스 응용	① (의료 공공) 합성 임상데이터, 합성 통계데이터 등		●	●	●	○	하	기타 검토기술
		② (금융) 동형암호(HE)/안전한 다자 연산(SMPC) 기반 자금세탁방지(AML)·고객신원확인(KYC) 분석		●	●	●	○	하	기타 검토기술
		③ (금융) 프라이버시 보호 신용평가 등		●	●	●	○	하	기타 검토기술
		④ (의료) 전자의무기록(EMR) 등의 PET 분석		●	●	●	○	하	기타 검토기술
		⑤ (공공) 차분 프라이버시를 적용하여 개인정보 위험을 낮춘 데이터 공개		●	●	●	○	하	기타 검토기술
		⑥ (일반) 생활속에서의 프라이버시 영상 보호(CCTV, 현관문 카메라 등)		●	●	●	○	하	기타 검토기술
		⑦ 기타 메타버스 환경 등에서의 프라이버시 보호		○	●	○	○	하	기타 검토기술
	3-3 마이데이터 기반기술	① 데이터 클린룸·데이터 스페이스 연계 PET		●	●	●	○	하	기타 검토기술
		② 마이데이터 동의·위임 통합 자동화 플랫폼		⊙	⊙	⊙	⊙	**상**	**핵심기술**
		③ 마이데이터-AI 개인정보 비서 연동·운영		●	●	●	●	하	기타 검토기술

중분류(4)	소분류(15)	세분류(59)	기준 ❶	기준 ❷	기준 ❸	기준 ❹	종합 판정	선정 단계
4 AI 대응 기술개발	4-1 AI 모델 학습단계 프라이버시	① 차분 프라이버시(DP) 적용 (LLM 파인튜닝 학습 프레임워크)	●	●	●	○	하	기타 검토기술
		② 언러닝(Unlearning)	●	●	●	○	하	기타 검토기술
		③ 연합학습 (FL, Federated Learning)	●	●	○	○	하	기타 검토기술
		④ 합성데이터 생성·정제·검증 (학습용)	●	●	●	○	하	기타 검토기술
	4-2 AI 모델 프라이버시 공격·방어 및 안전성 평가	① 정렬 파인튜닝(인간 피드백 기반 강화학습(RLHF)/선호신호 직접 최적화(DPO)/그룹 비교 정렬 최적화(GRPO))	○	●	○	○	하	기타 검토기술
		② AI 모델 안전성 평가	⦿	⦿	⦿	⦿	**상**	**핵심기술**
		③ 설명가능/감사가능 AI (XAI/Auditable AI)	●	●	●	○	하	기타 검토기술
		④ 실시간(데이터 스트림) 입·출력 가드레일	●	●	●	○	하	기타 검토기술
		⑤ 합성데이터 기반 학습·증강 (분포 정합/ 혼합비율 최적화)	●	●	●	○	하	기타 검토기술
	4-3 AI 콘텐츠 신뢰성·출처	① 콘텐츠 출처 및 진위 보장을 위한 국제 협의체(C2PA)/워터마킹 등 출처·이력 설계	●	○	⦿	○	중	후보기술
		② 생성 합성콘텐츠 탐지·표시 (실시간 경고·차단 포함)	●	●	⦿	○	중	후보기술
	4-4 AI 에이전트 보안	**① 에이전트·도구·로봇 실행 보안**	⦿	⦿	⦿	⦿	**상**	**핵심기술**
		② AI 개인정보 비서 운영 관련 표준 기반 연결 인터페이스(모델 컨텍스트 프로토콜(MCP))	●	●	●	○	하	기타 검토기술
		③ 피지컬 AI 실시간 프라이버시 제어	⦿	⦿	⦿	⦿	**상**	**핵심기술**
	4-5 AI 기반 개인정보 탐지·비식별화	① 코드 시크릿 탐지 엔진	●	●	●	●	하	기타 검토기술
		② 문서·이미지 음성 개인정보 탐지	●	●	●	●	하	기타 검토기술
		③ 멀티모달 개인정보 검출(비전-언어모델(VLM) 기반 크로스 모달)	●	●	●	○	하	기타 검토기술
		④ AI기반 정형데이터 비식별화	●	○	⦿	○	중	후보기술
		⑤ AI기반 비정형데이터 비식별화 (영상, 텍스트, 음성 등)	⦿	⦿	⦿	⦿	**상**	**핵심기술**
		⑥ 피지컬 AI/로봇 센싱 프라이버시	●	○	⦿	○	중	후보기술

11개 핵심기술은 사회적 현안을 해결하고, AI 등 신산업 환경에서도 시의성 있게 개인정보를 보호하면서 안전한 활용이 가능

중분류	소분류	핵심기술(세분류)	선정 필요성
1 개인정보 주권 보장	1-2 정보주체 통제권	① 정책 준수 증명 결과 열람	정보주체의 처리·열람·삭제 요청 등의 이력과 이행 여부를 확인이 어렵고, 요청결과에 대한 위·변조 방지 및 자동 확인이 가능한 통제기술 연구 필요
2 유·노출 위험 경감	2-1 수집 시 개인정보 탐지	② 딥페이크/합성 검증·레이블링	AI 기술로 영상 등 비정형데이터를 악의적으로 합성·조작하여 디지털 성범죄 등 사회문제가 발생하고 있으므로 이를 예방·해결하기 위한 기술연구 필요
	2-3 개인정보 안전성 확보	④ 엣지 디바이스 개인정보보호	PC·모바일·IoT 등 각종 단말기에서 개인정보 처리와 이에 따른 유출 위험이 높아져, 장치 내에서 이상행위를 탐지하고 즉시 차단하는 보호 기술연구 필요
	2-4 외부 유출 모니터링·탐지	① 다크웹·표면웹 유출 탐지	다크웹 등 음성화된 사이트를 통한 개인정보 유포로 2차 피해가 확대되고 있으므로, 불법 게시물·거래 정황을 조기 확인하고 확산경로를 추적하는 기술연구 필요
3 신뢰기반 안전활용	3-1 안전활용 기반기술	⑦ 재식별 위험도 평가·검증	가명·익명정보가 다른정보와 결합하여 개인이 재식별될 위험성이 있으므로, 객관적·정량적 수치로 평가 및 안전기준 충족 여부 확인하는 기술연구 필요
		⑧ 합성데이터 등 PET 기반 비식별화 (단일·하이브리드)	데이터 활용 수요 증가 대비 개인정보 침해 우려가 높아져, 분석·활용 성능은 유지하면서 재식별 가능성은 낮추는 비식별화 기술연구 필요
	3-3 마이데이터 기반기술	① 마이데이터 동의·위임 통합 자동화 플랫폼	마이데이터 확산에 따른 정보주체 권리행사(동의·위임·열람·이동·철회 등) 과정을 한 곳에서 확인·처리하고 변경사항을 자동 반영하는 자동화된 기술개발 필요
4 AI 대응 기술개발	4-2 AI 모델 공격·방어/안전성	② AI 모델 안전성 평가	AI 학습·추론·생성 과정에서 개인정보 노출과 신종 공격 위험이 증가하고 있어 공격 유형별 취약성을 시험하고 노출 가능성을 점검하는 평가기술 연구 필요
	4-4 AI 에이전트 보안	① 에이전트·도구·로봇 실행 보안	AI 에이전트가 외부 도구·서비스를 자동 호출 시, 과도한 권한 사용과 개인정보 오남용 위험이 커지고 있으므로 실행 전 권한 및 허용범위 내 작동하는 제어기술 연구 필요
		③ 피지컬 AI 실시간 프라이버시 제어	로봇·스마트기기 등에서 영상·음성·행동정보를 수집·이용함에 따라 개인정보 수집 범위·정밀도·보관기간을 즉시 조정·제어하는 실시간 보호 기술연구 필요
	4-5 AI 기반 개인정보 탐지·비식별화	⑤ AI 기반 비정형데이터 개인정보 탐지·비식별화	텍스트·영상·이미지·음성 등의 높은 활용 수요 대비 수작업에 따른 낮은 정확도와 속도 한계를 개선하는 고도화된 개인정보 자동 탐지·비식별화 기술연구 필요

2 최종 선정된 로드맵 대상 핵심기술 및 표준

최종 선정된 11개 핵심기술의 개념을 정의하고, 기술 연구개발을 추진하기 위한 세부적인 기술 및 이와 관련된 표준화 대상을 도출

최종 선정된 로드맵 대상 핵심 기술

중분류	소분류	핵심 기술(세분류)	개념 및 주요 세부 기술·표준	비고
1 개인정보 주권 보장	1-2 정보주체 통제권	① 정책 준수 증명 결과 열람	· **(개념)** 개인정보 처리·권리행사 이력을 위변조 방지 기술로 관리하고, 검색/열람/삭제 요청 이행 여부를 정책·법규 기준으로 자동 분석·증명해 정보주체에게 제공하는 기술 · **(세부 기술)** - 개인정보 활용 현황을 모니터링하고 통제권 실행을 보장하는 기술 - 검색증강생성(RAG) 프라이버시 기반 개인정보 보존형 검색(Retrieval) 및 실시간 삭제증명(Forget-by-Design) 기술 · **(관련 표준)** - [국제표준] 소비자 권리 보호를 위한 PbD(Privacy by Design) 관련 국제표준	
2 유·노출 위험 경감	2-1 수집 시 개인정보 탐지	② 딥페이크/합성 검증·레이블링	· **(개념)** 이미지·영상·음성의 딥페이크/합성 여부를 자동 판별해 메타데이터 및 화면 표시로 라벨링하는 기술 · **(세부 기술)** - 딥페이크 사전 예방을 위한 데이터 변환 기술* - 저위험 비식별 음성데이터 기반 보이스피싱·딥페이크 지능형 탐지·차단 및 안전활용 통합 기술 · **(관련 표준)** - [국제표준] 딥페이크·합성콘텐츠 진위검사 결과를 기록·공유하기 위한 공통 메타데이터 항목 및 화면 표시 방식 국제표준 - [국내표준] 유관 기관·서비스 간 딥페이크/합성콘텐츠 진위검사 결과를 안전하게 공유하기 위한 인터페이스·프로토콜 국내표준	* '26 예산 반영
	2-3 개인정보 안전성 확보	④ 엣지 디바이스 개인정보보호	· **(개념)** PC·모바일·IoT 등 엣지 단말에서 앱·프로세스 행위를 모니터링하고 격리/통제를 통해 단말 수준에서 개인정보 유출·오남용을 예방하기 위한 기술 · **(세부 기술)** - 온디바이스 격리 환경에서의 개인정보 이상행위 탐지 및 자동 통제 기술 · **(관련 표준)** - [국제표준] 엣지·모바일 단말 환경에서 개인정보 보호를 위한 보안 아키텍처·접근통제 요구사항 국제표준 - [국내표준] 온디바이스 개인정보 이상행위 탐지·차단 기능 및 로그 관리에 관한 시험·평가기준 국내표준	

중분류	소분류	핵심 기술(세분류)	개념 및 주요 세부 기술·표준	비고
2 유·노출 위험 경감	2-4 외부 유출 모니터링·탐지	① 다크웹·표면웹 유출 탐지	· **(개념)** 다크웹·표면웹에서 수집한 정보를 분석해 개인정보 불법 유출 및 거래 정황을 탐지·추적하는 기술 · **(세부 기술)** - 다크웹 상 개인정보 불법유통 패턴 분석 및 공급망 위험지수 산출 기술 - 도메인명·IP 주소 범위를 기반으로 한 노출 자산 네트워크 스캐닝 및 취약점 식별 기술 - 유출 탐지 시스템의 성능 평가 지표·시험방법 및 보고서 템플릿 설계·검증 기술 · **(관련 표준)** - [국제표준] 다크웹·표면웹 인텔리전스(OSINT) 수집·교환 포맷 및 기관 간 연계 인터페이스 국제표준 - [국내표준] 개인정보 유출 탐지·분류·신고를 위한 공통 데이터 모델 및 API 국내표준 규격	
3 신뢰기반 안전활용	3-1 안전활용 기반기술	⑦ 재식별 위험도 평가·검증	· **(개념)** 가명·비식별 데이터의 재식별 가능성을 정량 산정하고 안전성 기준 충족 여부를 검증하는 기술 · **(세부 기술)** - 비정형 합성데이터의 안전성 검증 및 유용성 평가 기술* - 가명 익명정보 재식별 검증 기술* - PC·모바일의 기기식별자 등 운용 현황 분석 및 웹스크래핑 상황의 개인정보 재식별 위험 판단, 개인정보 통제 기술 · **(관련 표준)** - [국내표준] 가명·비식별 정보 재식별 위험도 평가 방법론 및 지표에 관한 국가표준(KS) - [국내표준] 비식별 데이터의 안전성 등급 분류 및 재식별 위험 검증 절차·보고서 형식 국내표준	* '26 예산 반영
		⑧ 합성데이터 등 PET 기반 비식별화(단일·하이브리드)	· **(개념)** 합성데이터 등 각종 프라이버시 강화 기술(PET)들을 단일 혹은 조합하여 활용도는 유지하면서 재식별 위험을 허용 수준 이하로 낮추는 비식별화 기술 · **(세부 기술)** - 개인정보 보유기간 제한을 고려한 시계열 합성데이터 생성 및 검증 기술* · **(관련 표준)** - [국제표준] 학습·분석용 합성데이터의 품질·프라이버시· 유용성 평가 기준 및 시험방법 국제표준 - [국내표준] 합성데이터·차분 프라이버시·가명처리 등 PET 연계 비식별 처리 프로파일·참조모델 국내 표준	* '26 예산 반영

중분류	소분류	핵심 기술(세분류)	개념 및 주요 세부 기술·표준	비고
3 신뢰기반 안전활용	3-3 마이데이터 기반기술	① 마이데이터 동의·위임 통합 자동화 플랫폼	· **(개념)** 마이데이터 환경에서 정보주체의 동의·위임·열람·삭제·이동권을 통합 관리하고, 분산신원(DID)과 자기주권신원(SSI) 기반 지갑과 연계하여 신원·자격·개인정보 제공·철회 흐름을 통합 자동화하는 플랫폼 기술 · **(세부 기술)** - 마이데이터·공공 서비스 연계를 위한 SSI 기반 개인정보 지갑 레퍼런스 구현 및 운영 보안 검증 기술 · **(관련 표준)** - [국제표준] 마이데이터 서비스의 정보주체 권리 및 통제권 보장을 위한 국제표준	
4 AI 대응 기술개발	4-2 AI 모델 공격·방어/안전성	② AI 모델 안전성 평가	· **(개념)** AI 모델에 대한 멤버십·속성추론·인버전·프롬프트 공격을 방어하고, 개인정보 노출·편향·취약성을 지표와 시험 시나리오로 평가/인증하는 기술 · **(세부 기술)** - 파운데이션 모델 학습데이터의 프라이버시 리스크 관리 기술* - 파운데이션 모델 운용 과정에서 민감정보 추론 방지 기술* - 생성형 AI 모델의 프라이버시 취약성 평가 및 개인정보 생성 억제(성능 저하 최소화) 기술* - 선택적 언러닝 및 검증 가능한 모델 수준 개인정보 삭제·파기 기술 · **(관련 표준)** - [국제표준] 파운데이션 모델 학습데이터 프라이버시 리스크 평가·완화 가이드라인 및 요구사항 국제표준 - [국제표준] 개인정보·편향·보안을 포함한 AI 모델 안전성 평가 지표·벤치마크 및 시험방법 국제표준	* '25, '26 예산 반영
	4-4 AI 에이전트 보안	① 에이전트·도구·로봇 실행 보안	· **(개념)** AI 에이전트의 도구·API 호출 시 사용자 신원·역할·동의와 연계된 권한과 실행 조건을 제어해 개인정보 오남용과 침해를 방지하는 기술 · **(세부 기술)** - 에이전틱 AI 기반 개인정보 전 생애주기 자동 거버넌스 및 위험예측·보호조치 기술 - 멀티모달 맥락 인식 기반 개인용 프라이버시 코파일럿: 트랜스포머·AI 에이전트를 활용한 다채널 개인정보 유출 점검·상담 자동화 기술 개발 - PET 조합 기반 에이전틱/피지컬 AI 행동정책 설계·검증 및 프라이버시 보존 실행엔진 기술 - 에이전트 계정·지갑(SSI/DID 등)과 연계된 사용자 신원·권한·동의 관리를 통한 안전한 실행 통제 기술 · **(관련 표준)** - [국제표준] AI 에이전트 권한·정책 언어 및 정책 집행·신원 연계 인터페이스 국제표준 - [국내표준] 에이전트-도구/플러그인 연계 시 보안·프라이버시 요구사항 및 권한·동의 위임 모델 국내표준	

중분류	소분류	핵심 기술(세분류)	개념 및 주요 세부 기술·표준	비고
4 AI 대응 기술개발	4-4 AI 에이전트 보안	③ 피지컬 AI 실시간 프라이버시 제어	· **(개념)** 로봇·IoT·스마트기기의 센싱·전송·저장 과정에서 수집 범위·해상도· 보존기간 등을 제어해 실시간 프라이버시를 보호하는 기술 · **(세부 기술)** - 피지컬 AI·로봇 융합 환경을 위한 프라이버시 인지형 신원·행동 관리 및 최소수집 기술 - 로봇·IoT 등 실환경에서 개인정보 안전교환 프로토콜 및 상호작용 기술 · **(관련 표준)** - [국제표준] 로봇·IoT·스마트기기의 센싱·저장·전송 단계별 프라이버시 보호 설계·운영 가이드라인 국제표준 - [국내표준] 피지컬 AI 서비스에 대한 프라이버시 영향평가(PIA)·위험등급 분류 및 인증 기준 국내표준	
	4-5 AI 기반 개인정보 탐지·비식별화	⑤ AI 기반 비정형데이터 개인정보 탐지·비식별화	· **(개념)** 텍스트·영상·이미지·음성 등 멀티모달 환경에서 트랜스포머 등 AI 모델을 활용한 이름·주소·얼굴·번호 등 다양한 개인정보를 문맥 기반으로 탐지·비식별화하는 기술 · **(세부 기술)** - 멀티모달형 AI 기반 개인정보 탐지 추적 및 비식별화 기술* - 트랜스포머 기반 텍스트 개인정보 탐지 및 한국어·다국어 파운데이션 모델·오픈소스 라이브러리 개발 기술 · **(관련 표준)** - [국제표준] AI 기반 비정형데이터 개인정보 탐지·비식별화 성능 평가용 벤치마크·지표·시험방법 국제표준 - [국내표준] 로그·대화·비정형데이터 개인정보 탐지·비식별 결과 공통 포맷·연계 인터페이스 국내표준	* '26 예산 반영

※ 위 표에서 (관련 표준)은 해당 기술과 연계될 국내/국제 표준안·기술규격의 목표 수준을 의미함

※ 국제표준: ISO/IEC, IEEE 등 / 국내표준: TTA, KS 등

VI 중점 추진과제

1. 기술개발 및 표준화 로드맵
2. 세부 추진방안

CHAPTER VI

중점 추진과제

1 기술개발 및 표준화 로드맵

(범례) : 세부 기술 : 표준

중분류	소분류	핵심 기술	2026	2027	2028	2029	2030
1 개인정보 주권 보장	1-2 정보주체 통제권	① 정책 준수 증명 결과 열람		개인정보 활용 현황을 모니터링하고 통제권 실행 을 보장하는 기술			
				검색증강생성(RAG) 프라이버시 기반 개인정보 보존형 검색(Retrieval) 및 실시간 삭제 증명(Forget-by-Design) 기술			
			[국제표준] 소비자 권리 보호를 위한 PbD 관련 국제표준				
2 유·노출 위험 경감	2-1 수집 시 개인정보 탐지	② 딥페이크/합성 검증·레이블링	딥페이크 사전 예방을 위한 데이터 변환 기술				
				저위험 비식별 음성데이터 기반 보이스피싱·딥페이크 지능형 탐지·차단 및 안전활용 통합 기술			
				[국제표준] 딥페이크·합성콘텐츠 진위검사 결과를 기록·공유하기 위한 공통 메타데이터 항목 및 화면 표시 방식 국제표준			
				[국내표준] 유관 기관·서비스 간 딥페이크/합성콘텐츠 진위검사 결과를 안전하게 공유하기 위한 인터페이스·프로토콜 국내표준			
	2-3 개인정보 안전성 확보	④ 엣지 디바이스 개인정보보호		온디바이스 격리 환경에서의 개인정보 이상행위 탐지 및 자동 통제 기술			
					[국제표준] 엣지·모바일 단말 환경에서 개인정보보호를 위한 보안 아키텍처·접근통제 요구사항 국제표준		
					[국내표준] 온디바이스 개인정보 이상행위 탐지·차단 기능 및 로그 관리에 관한 시험·평가기준 국내 표준		

중분류	소분류	핵심 기술	2026	2027	2028	2029	2030
2 유·노출 위험 경감	**2**-4 외부 유출 모니터링·탐지	① 다크웹·표면웹 유출 탐지		다크웹 상 개인정보 불법유통 패턴 분석 및 공급망 위험지수 산출 기술			
					도메인명·IP 주소 범위를 기반으로 한 노출 자산 네트워크 스캐닝 및 취약점 식별 기술		
					유출 탐지 시스템의 성능 평가 지표·시험방법 및 보고서 템플릿 설계·검증 기술		
					[국제표준] 다크웹·표면웹 인텔리전스(OSINT) 수집·교환 포맷 및 기관 간 연계 인터페이스 국제표준		
					[국내표준] 개인정보 유출 탐지·분류·신고를 위한 공통 데이터 모델 및 API 국내표준 규격		
3 신뢰기반 안전활용	**3**-1 안전활용 기반기술	⑦ 재식별 위험도 평가 검증	비정형 합성데이터의 안전성 검증 및 유용성 평가 기술				
			가명 익명정보 재식별 검증 기술				
					PC·모바일의 기기식별자 등 운용 현황 분석 및 웹스크래핑 상황의 개인정보 재식별 위험 판단, 개인정보 통제 기술		
					[국내표준] 가명·비식별 정보 재식별 위험도 평가 방법론 및 지표에 관한 국가표준		
					[국내표준] 비식별 데이터의 안전성 등급 분류 및 재식별 위험 검증 절차·보고서 형식 국내표준		
		⑧ 합성데이터 등 PET 기반 비식별화(단일·하이브리드)	개인정보 보유기간 제한을 고려한 시계열 합성데이터 생성 및 검증 기술				
					[국제표준] 학습·분석용 합성데이터의 품질·프라이버시·유용성 평가 기준 및 시험방법 국제표준		
					[국내표준] 합성데이터·차분 프라이버시·가명처리 등 PET 연계 비식별 처리 프로파일·참조모델 국내표준		
	3-3 마이데이터 기반기술	① 마이데이터 동의·위임 통합 자동화 플랫폼			마이데이터·공공 서비스 연계를 위한 SSI 기반 개인정보 지갑 레퍼런스 구현 및 운영 보안 검증 기술		
				[국제표준] 마이데이터 서비스의 정보주체 권리 및 통제권 보장을 위한 국제표준			

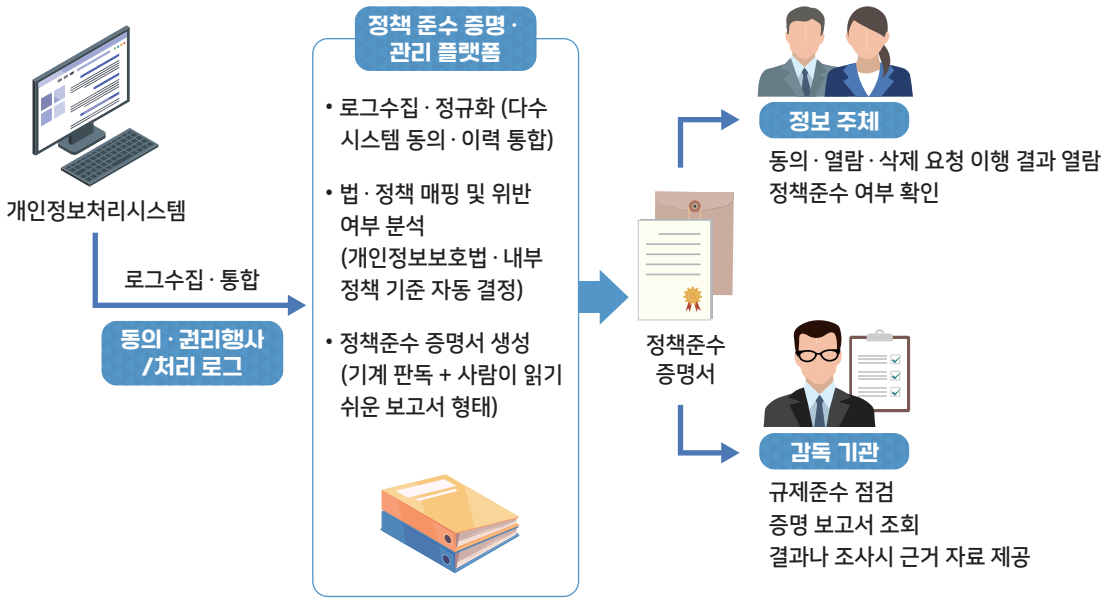
중분류	소분류	핵심 기술	2026	2027	2028	2029	2030
4 AI 대응 기술개발	4-2 AI 모델 공격·방어/안전성	② AI 모델 안전성 평가	파운데이션 모델 학습데이터의 프라이버시 리스크 관리 기술				
			파운데이션 모델 운용 과정에서 민감정보 추론 방지 기술				
			생성형 AI 모델의 프라이버시 취약성 평가 및 개인정보 생성 억제 기술(성능 저하 최소화)				
				선택적 언러닝 및 검증 가능한 모델에서의 개인정보 삭제·파기 기술			
					[국제표준] 파운데이션 모델 학습데이터 프라이버시 리스크 평가·완화 가이드라인 및 요구사항 국제표준		
					[국제표준] 개인정보·편향·보안을 포함한 AI 모델 안전성 평가 지표·벤치마크 및 시험방법 국제표준		
	4-4 AI 에이전트 보안	① 에이전트·도구·로봇 실행 보안		에이전틱 AI 기반 개인정보 전 생애주기 자동 거버넌스 및 위험예측·보호조치 기술			
				멀티모달 맥락 인식 기반 개인용 프라이버시 코파일럿: 트랜스포머·AI 에이전트를 활용한 다채널 개인정보 유출 점검·상담 자동화 기술			
				PET 조합 기반 Agentic/Physical AI 행동 정책 설계·검증 및 프라이버시 보존 실행엔진 기술			
					에이전트 계정·지갑(SSI/DID 등)과 연계된 사용자 신원·권한·동의 관리를 통한 안전한 실행 통제 기술		
				[국제표준] AI 에이전트 권한·정책 언어 및 정책 집행·신원 연계 인터페이스 국제표준			
				[국내표준] 에이전트-도구/플러그인 연계 시 보안·프라이버시 요구사항 및 권한·동의 위임 모델 국내 표준			

<table>
<tr><th>중분류</th><th>소분류</th><th>핵심 기술</th><th>2026</th><th>2027</th><th>2028</th><th>2029</th><th>2030</th></tr>
<tr><td rowspan="6">4 AI 대응 기술개발</td><td rowspan="3">4-4
AI 에이전트 보안</td><td rowspan="3">③ 피지컬 AI 실시간 프라이버시 제어</td><td colspan="3">피지컬 AI·로봇 융합 환경을 위한 프라이버시 인지형 신원·행동 관리 및 최소수집 기술</td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="3">로봇·IoT 등 실환경에서 개인정보 안전교환 프로토콜 및 상호작용 기술</td></tr>
<tr><td colspan="2"></td><td colspan="3">[국제표준] 로봇·IoT·스마트기기의 센싱·저장·전송 단계별 프라이버시 보호 설계·운영 가이드라인 국제표준</td></tr>
<tr><td colspan="2"></td><td colspan="3">[국내표준] 피지컬 AI 서비스에 대한 프라이버시 영향평가(PIA)·위험등급 분류 및 인증 기준 국내표준</td></tr>
<tr><td rowspan="3">4-5
AI 기반 개인정보 탐지·비식별화</td><td rowspan="3">⑤ AI 기반 비정형데이터 개인정보 탐지·비식별화</td><td colspan="2">멀티모달형 AI 기반 개인정보 탐지 추적 및 비식별화 기술</td><td colspan="3"></td></tr>
<tr><td colspan="2"></td><td colspan="3">트랜스포머 기반 텍스트 개인정보 탐지 및 한국어·다국어 개인정보 탐지용 파운데이션 모델·오픈소스 라이브러리 개발 기술</td></tr>
<tr><td colspan="2"></td><td colspan="3">[국제표준] AI 기반 비정형데이터 개인정보 탐지·비식별화 성능 평가용 벤치마크·지표·시험방법 국제표준</td></tr>
<tr><td colspan="2"></td><td colspan="3">[국내표준] 로그·대화·비정형데이터 개인정보 탐지·비식별 결과 공통 포맷·연계 인터페이스 국내표준</td></tr>
</table>

※ 연도 별 신규 예산확보 여건에 따라 연구개발 추진시점 등은 일부 변경가능

2 세부 추진방안

1. 정책 준수 증명 결과 열람



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
정책 준수 증명 결과 열람		개인정보 활용 현황을 모니터링하고 통제권 실행을 보장하는 기술			
		검색증강생성(RAG) 프라이버시 기반 개인정보 보존형 검색(Retrieval) 및 실시간 삭제증명 (Forget-by-Design) 기술			
	[국제표준] 소비자 권리 보호를 위한 PbD 관련 표준				

기술 세부내용

- 개인정보 활용 현황을 모니터링하고 권리행사에 필요한 통제권 실행 운영·기술
  - 글로벌 위협에 대응하는 개인정보 전주기 모니터링 및 자율 통제 기술로 개인정보 활용현황을 통합 수집·시각화 및 정책준수 증명 플랫폼 개발
  - 열람·정정·삭제·전송요구·처리정지 등 정보주체 권리행사를 위한 통합 자동화 및 실행 보장 엔진 개발
  - 감사·규제 대응을 위한 활용·권리행사 이력 관리 및 위험 기반 통제 정책 엔진 개발

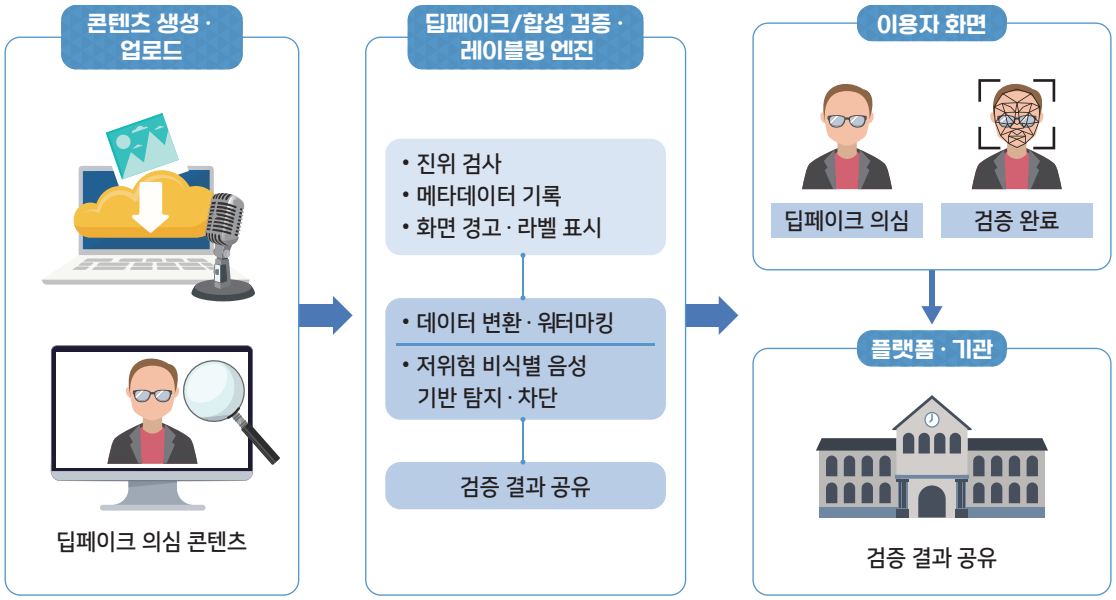
- 검색증강생성(RAG) 프라이버시 기반 보존형 검색(Retrieval) 및 실시간 삭제증명(Forget-by-Design) 기술
  - 검색증강생성(RAG) 구조에서 민감정보를 보호하면서 개인정보 검색·조회를 지원
  - 시스템 상에서 인덱스·캐시·로그 등에서 개인정보가 실제로 제거되었는지 여부 등을 확인하고, 삭제증명에 필요한 토큰·로깅 정보를 생성

표준화 추진

- [국제표준] 소비자 권리 보호를 위한 PbD(Privacy by Design) 표준
  - 권리행사 및 정책준수의 검증 가능한 증명을 위해, 이력·로그의 관리 기준(보관기간·무결성·접근통제)과 증명 데이터 형식·검증 절차를 표준화
  - 동의·처리·삭제, 제3자 제공 등 핵심요소에 대한 공통 데이터 모델·연계 인터페이스를 정의하고 투명성 등을 요구사항을 국제 표준화

- [국내표준] 국내 기준 정비를 통해 국제표준으로 연계
  - 국내 운용 중인 개인정보 보관·관리 SW·HW 관련, 이력·로깅·삭제증명·제3자 제공 기능 등에 대한 요구사항 및 참조모델을 표준 항목화
  - 권리행사 및 정책준수 증명에 필수적인 요구사항과 항목 등을 정의하고, SW·HW의 실증·검증 결과를 반영하여 PbD 기반 국제표준으로 연계·추진

2. 딥페이크/합성 검증·레이블링



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
딥페이크/합성 검증·레이블링	딥페이크 사전 예방을 위한 데이터 변환 기술				
		저위험 비식별 음성데이터 기반 보이스피싱·딥페이크 지능형 탐지·차단 및 안전활용 통합 기술			
		[국제표준] 딥페이크·합성콘텐츠 진위검사 결과를 기록·공유하기 위한 공통 메타데이터 항목 및 화면 표시 방식 국제표준			
		[국내표준] 유관 기관·서비스 간 딥페이크/합성콘텐츠 진위검사 결과를 안전하게 공유하기 위한 인터페이스·프로토콜 국내표준			

기술 세부내용

- 딥페이크 사전 예방형 데이터 변환 기술
  - 이미지·영상·음성에 워터마크·노이즈 삽입 등 사전 변환기술 적용
  - 진위검사 시, 변환기술을 통한 합성·위변조 여부를 자동 판별
  - 실시간으로 플랫폼·서비스 내 경고·표시·차단 정책과 연계·활용

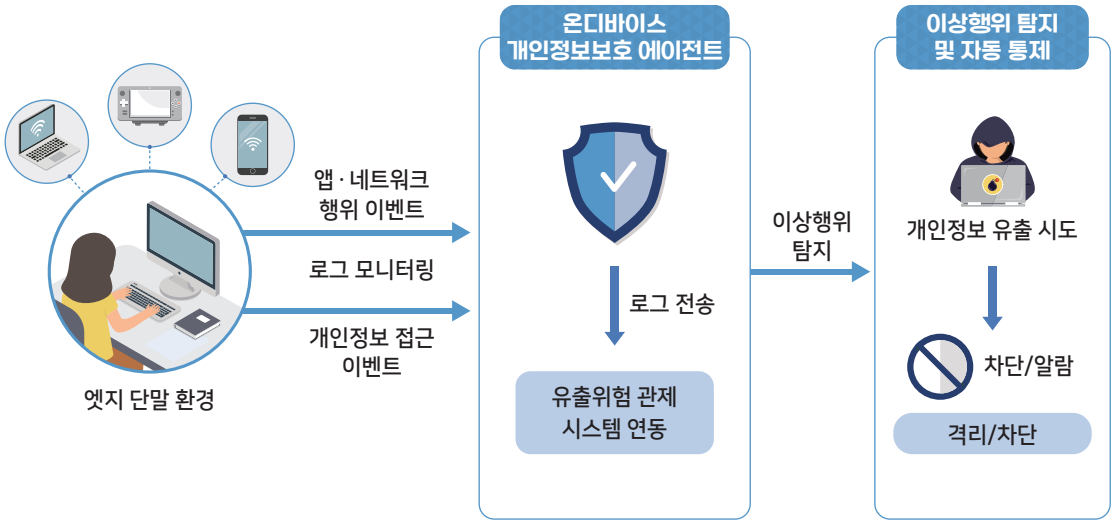
- 저위험 비식별 음성데이터 기반 보이스피싱·딥페이크 지능형 탐지·차단·안전활용 통합 기술
  - 비식별 처리된 음성정보를 보이스피싱·음성 딥페이크 패턴으로 학습
  - 콜센터, 통신 망·앱 등에서 의심 통화·음성 합성을 자동 탐지·차단
  - 탐지 결과를 모델 고도화 및 통계 분석으로 안전하게 활용할 수 있도록 통합 지원

표준화 추진

- [국제표준] 딥페이크·합성콘텐츠 진위검사 결과 메타데이터·표시 방식 정의
  - 콘텐츠 진위 여부 관련, '판별결과, 신뢰도, 검사 시각, 검사 주체 등'을 포함하는 활용 가능한 공통 형식의 메타데이터의 필드 등을 정립
  - 정보주체 등 이용자의 화면표시 규격(아이콘, 문구, 경고창 등)에 대한 기본 가이드라인을 국제표준으로 제안 병행

- [국내표준] 진위검사 결과 공유 인터페이스·프로토콜 표준화
  - 플랫폼 사, 수사·규제기관, 언론·방송계, 보안기업 등 진위검사 관련 연계 수요가 있는 유관기관 간 송수신하는 API·포맷 규격 정의
  - 진위검사 결과 전송 시 보안(암호화)·무결성·접근통제 요구사항을 포함한 국내 환경에 적합한 인터페이스·프로토콜의 표준화 추진

3. 엣지 디바이스 개인정보보호



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
엣지 디바이스 개인정보보호		온디바이스 격리 환경에서의 개인정보 이상행위 탐지 및 자동 통제 기술			
			[국제표준] 엣지·모바일 단말 환경에서 개인정보 보호를 위한 보안 아키텍처·접근통제 요구사항 국제표준		
			[국내표준] 온디바이스 개인정보 이상행위 탐지·차단 기능 및 로그 관리에 관한 시험·평가기준 국내표준		

기술 세부내용

- 온디바이스 내 개인정보 이상행위 탐지 및 자동 통제 기술
  - PC·모바일·IoT 등 각종 단말장치(Device) 내에서 자체적으로 구동되는 앱(App)·프로세스·네트워크 관련 데이터를 실시간 수준의 모니터링
  - 일상적인 운영 환경의 보안 정책·패턴과 비교하여 개인정보 유출 시도·과도 수집·전송 등 악성 및 이상 행위에 대한 자동 탐지·통제
  - 이상 징후 발생 시, 프로세스 격리·통신 차단·추가 인증 요구·사용자 경고를 자동 수행

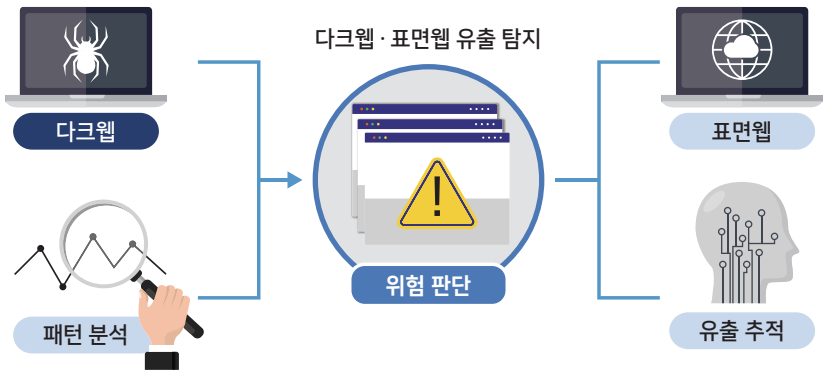
표준화 추진

- [국제표준] 엣지·모바일 단말의 개인정보보호 아키텍처·접근통제 요구사항 정의
  - 단말 기기 내 개인정보 저장 영역 분리, 최소권한 원칙, 앱·프로세스 격리 실행, 네트워크 제어 등 필수 요구사항 정의
  - 엣지·모바일 환경에서 개인정보 보호를 위한 기본 아키텍처·접근통제 요구사항을 국제적으로 통용되는 안내서로 규정 추진

- [국내표준] 온디바이스 개인정보 이상행위 탐지·차단 및 로그관리 시험·평가기준 정립
  - 단말장치 내 탑재되는 온디바이스 개인정보 보호 기능과 관련하여 공격을 탐지·차단하는 데 필요한 이상행위 유형과 성능 등*을 정의

    * 개인정보 등 비정상적 데이터 접근행위 판단 및 분석 수준, 탐지율·오탐율·처리시간 등
  - 유출 위협 분석·차단에 필요한 각종 로그의 저장·관리·제출 등 방법론 및 시험·검증에 필요한 평가기준을 국내 표준화 추진

4. 다크웹·표면웹 유출 탐지



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
다크웹·표면웹 유출 탐지		다크웹 상 개인정보 불법유통 패턴 분석 및 공급망 위험지수 산출 기술 개발			
			도메인명·IP 주소 범위를 기반으로 한 노출 자산 네트워크 스캐닝 및 취약점 식별 기술		
			유출 탐지 시스템의 성능 평가 지표·시험방법 및 보고서 템플릿 설계·검증 기술		
			[국제표준] 다크웹·표면웹 인텔리전스(OSINT) 수집·교환 포맷 및 기관 간 연계 인터페이스 국제표준		
			[국내표준] 개인정보 유출 탐지·분류·신고를 위한 공통 데이터 모델 및 API 국내 표준 규격		

기술 세부내용

- 다크웹 상 개인정보 불법유통 패턴 분석 및 공급망(Supply Chain) 위험지수 산출 기술
  - 다크웹 등 음성화된 사이트에서 데이터 수집·정규화 기술 및 글로벌 위협 대응 인텔리전스 연계 및 분석 엔진 개발
  - 개인정보 불법유통 패턴·공격 분석, 공격자 및 계정·도메인 등 위협 대상 식별 및 공급망 연계 분석 기술
  - 국가 공급망 체계 내 개인정보 유출 위험지수 산출 및 예·경보 대응 연계 기술 개발

- 기관 등의 보유 도메인·IP 대역을 기반으로 외부 노출 자산을 자동 탐색 및 유출 위험 등 취약 요소를 식별·조치하는 기술
  - 국가 차원의 개인정보 유출 위험 예측·탐지·예경보 체계 구축을 위하여 기관·기업 보유 자산의 외부 노출 여부, 취약점 등을 식별하고 사전 위험분석하는 기술*

  * 다량의 해외 유입 트래픽 대상으로 개인정보 유출시도를 예방하는 전처리 기술(비식별화 등) 포함

  - 관리 콘솔·저장소·테스트 서버 등 노출 자산과 주요 취약점 진단

- 개인정보 보호 시스템의 탐지 성능평가 지표·시험방법·보고서 템플릿* 설계 및 검증 기술

  * 시험 환경·데이터셋·시나리오, 지표 산출식 및 임계값, 탐지·오탐·대응시간 결과, 재현성 정보(버전·설정), 한계·위험요인, 개선 권고사항 등을 포함하는 공통 서식

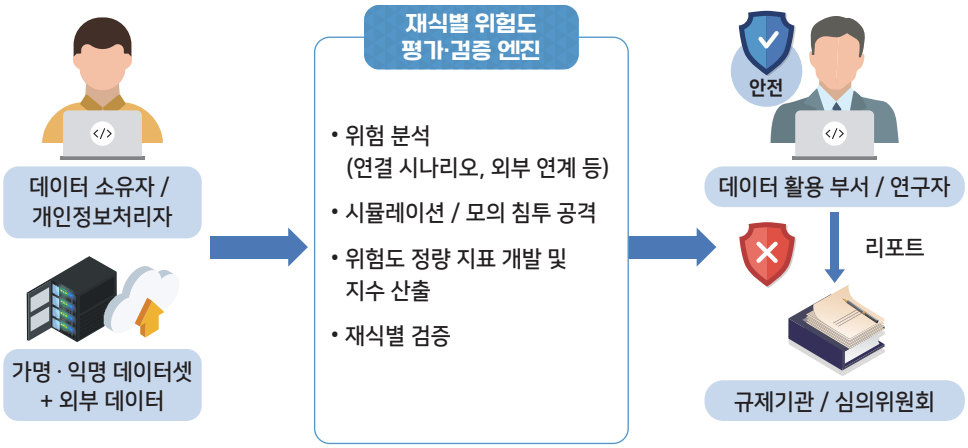
  - 개인정보 처리시스템 공격 탐지율, 오탐율, 대응시간 등 핵심 지표 정의
  - 범용성 있는 시험 및 시나리오 구성와 결과 보고서 템플릿 설계·검증

표준화 추진

- [국제표준] 다크웹·표면웹 내 확인가능한 공개출처정보(OSINT) 수집·교환 규격(format) 및 기관 연계용 인터페이스 정의
  - 수집한 데이터의 공통 필드(출처, 시간, 위험도 등)의 구조 정의 및 분석·조사 등 유관기관 간 협력을 위한 API·연계 절차 등 규격화

- [국내표준] 개인정보 유출 탐지·분류·신고를 위한 범용성있는 데이터 모델 정의 및 API 표준 규격
  - 유출 시도 유형 및 탐지, 영향도, 조치사항 등을 표현하는 공통된 규격의 데이터 모델 정의
  - 개인정보 처리시스템을 모니터링하는 전용 탐지 시스템과 조사·수사·분석·탐지 등 유관기관의 시스템 간 연계를 위한 API 규격 제정

5. 재식별 위험도 평가·검증



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
재식별 위험도 평가·검증	비정형 합성데이터의 안전성 검증 및 유용성 평가 기술				
	가명 익명정보 재식별 검증 기술				
			PC·모바일의 기기식별자 등 운용 현황 분석 및 웹스크래핑 상황의 개인정보 재식별 위험 판단, 개인정보 통제 기술 개발		
			[국내표준] 가명·비식별 정보 재식별 위험도 평가 방법론 및 지표에 관한 국가표준		
			[국내표준] 비식별 데이터의 안전성 등급 분류 및 재식별 위험 검증 절차·보고서 형식 표준		

기술 세부내용

- 비정형 합성데이터의 안전성 검증 및 유용성 평가 기술
  - 정형(텍스트 등), 비정형(이미지·영상·음성 등) 합성데이터에 대한 개인정보 재식별 위험지표 산출 및 분석·학습 활용성 지표 간 비교·평가

- 가명·익명정보 재식별 검증 기술
  - 외부 데이터와 결합·매칭(연계)을 통해 재식별 공격 시나리오를 설계하여 위험성 검증
  - 실험 결과를 바탕으로 재식별 성공률 및 잔여 재식별 위험도를 정량화 및 시각화하여 결과를 검증·확인하는 기술

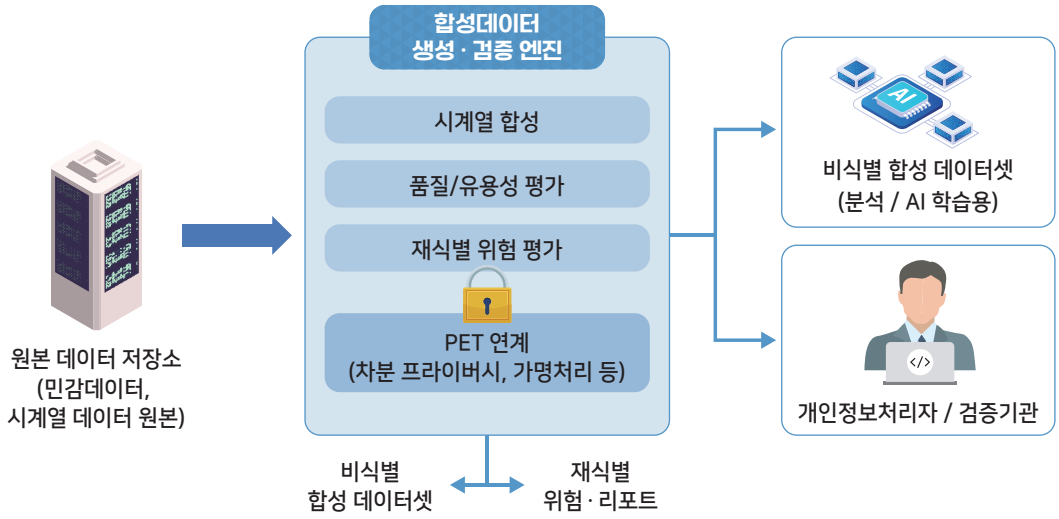
- PC·모바일 등 단말기에서 관리하는 기기식별자·웹스크래핑 기반의 재식별 위험 판단·통제 기술
  - 웹 브라우저를 통해 전송·관리되는 '쿠키, 광고ID, 디바이스ID, 웹스크래핑 로그 등'을 분석하는 기술
  - 분석 결과를 바탕으로 재식별 위험도를 상시적으로 수치화하고, 위험도에 따라 저감·통제하는 기술

표준화 추진

- [국제표준] 개인정보 재식별 위험도 평가 방법론·지표에 관한 표준
  - 글로벌 수준의 재식별 공격 유형·평가 절차·위험도 등 산정방식 정의
  - 범용성 높은 지표 정의 및 분석 결과를 해석·등급화 하는 등의 세분 기준을 규격화

- [국내표준] 재식별 위험에 대한 안전성 등급화 방법론 및 분류·검증절차·보고서 형식 등을 표준화
  - 재식별에 따른 파급력이 높은 고위험 분야 등을 정의하고 각 분야 별 데이터 안전성 등급 구간·판정 기준을 정의
  - 검증 방법론 개발을 통해 세부 절차와 결과 보고서 템플릿(항목·규격)을 국내 환경에 적합하게 표준화

6. 합성데이터 등 PET 기반(단일·하이브리드) 비식별화



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
합성데이터 등 PET 기반 비식별화 (단일·하이브리드)	개인정보 보유기간 제한을 고려한 시계열 합성데이터 생성 및 검증 기술				
			[국제표준] 학습·분석용 합성데이터의 품질·프라이버시·유용성 평가 기준 및 시험방법 국제표준		
			[국내표준] 합성데이터·차분 프라이버시·가명처리 등 PET 연계 비식별 처리 프로파일·참조모델 국내표준		

기술 세부내용

- 개인정보 보유기간 제한을 고려한 시계열 합성데이터 생성 및 검증 기술
  - 보유기간·보존주기 등을 반영한 시계열 합성데이터 생성 기법 설계
  - 원본 대비 통계·패턴 유지(유용성 관점) 및 합성데이터의 개인정보 재식별 위험도 관련 검증 병행
  - '차분 프라이버시, 가명처리 기술 등' 다양한 PET와 결합하여 비식별화의 수준 및 강도·활용도 균형 최적화

표준화 추진

- [국제표준] 학습·분석용 합성데이터 품질·프라이버시·유용성 평가 기준·시험방법 등 표준화
  - 합성데이터의 품질 및 프라이버시 지표, 유용성 지표를 평가하는 지표·시험 절차를 글로벌 수준으로 주도

※ (품질) 분포 정합도, 통계 유사도 등, (프라이버시) 재식별·누설 위험 등, (유용성) 모델 성능, 분석 정확도 등

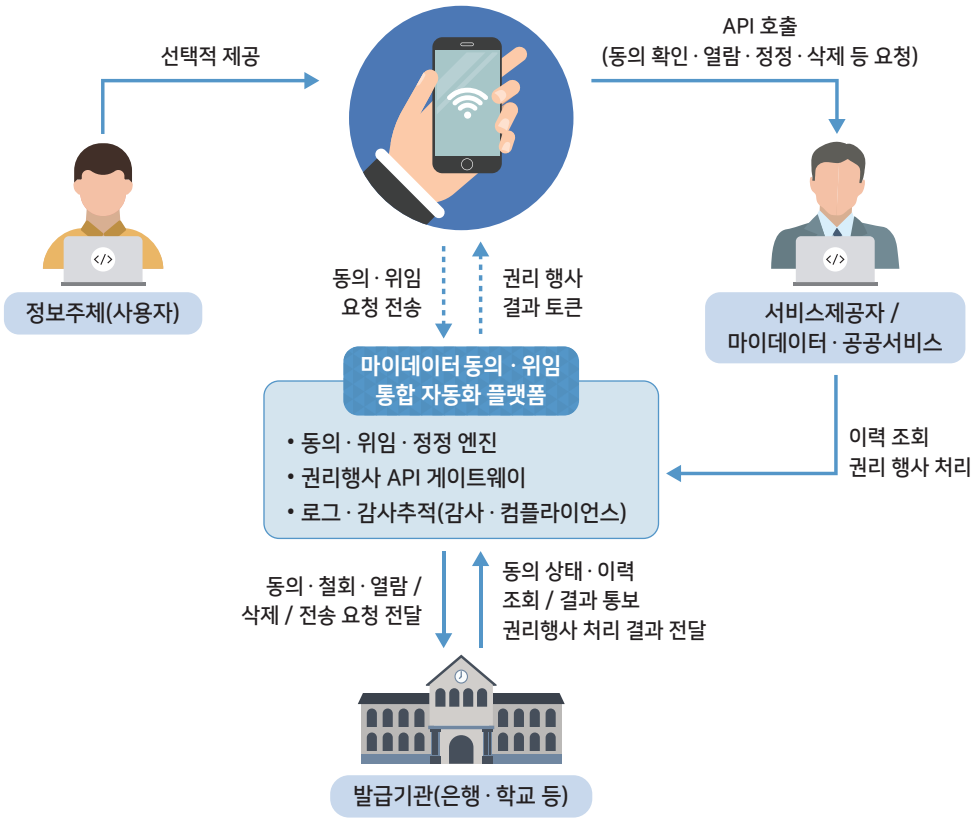
- [국내표준] 합성데이터·차분 프라이버시·가명처리 기술 등 PET 연계 비식별 처리 프로파일·참조모델 구성
  - 융합된 PET 적용 방법론 정의 및 참조 아키텍처 정의

※ (예시) 2개 이상의 PET 적용시 '순서, 조합, 설정 임계값 등'에 대한 안내 등을 포함

  - PET 적용 시 활용목적 및 공개범위* 별로 안전성·유용성 수준이 상이하므로, 적합한 권장 프로파일·구성 방법 정의 및 표준화

* 통계 결과의 외부 공개, 학습·분석용 데이터의 기관 간 공유 등

7. 마이데이터 동의·위임 통합 자동화 플랫폼



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
마이데이터 동의·위임 통합 자동화 플랫폼			마이데이터·공공 서비스 연계를 위한 SSI 기반 개인정보 지갑 레퍼런스 구현 및 운영 보안 검증 기술		
		[국제표준] 마이데이터 서비스의 정보주체 권리 및 통제권 보장을 위한 국제표준			

기술 세부내용

- 자기주권신원(SSI, Self-Sovereign Identity) 기반 개인정보 지갑 레퍼런스 구현 및 연계·보안 검증
  - 탈중앙화 식별자(DID)·검증가능한 자격증명(VC) 기반 개인정보 지갑 프로토타입 구현(발급·저장·제출·철회 기능 등)
  - 마이데이터·공공 서비스와의 연동 API·시나리오 설계 및 개인정보 보호 체계, 실 운영 환경 등을 검증하는 기술
  - 사용자가 직접 동의·제공 범위를 선택·철회할 수 있는 사용자 인터페이스(UI) 및 기술적·관리적 보호 정책과의 연계 체계 마련

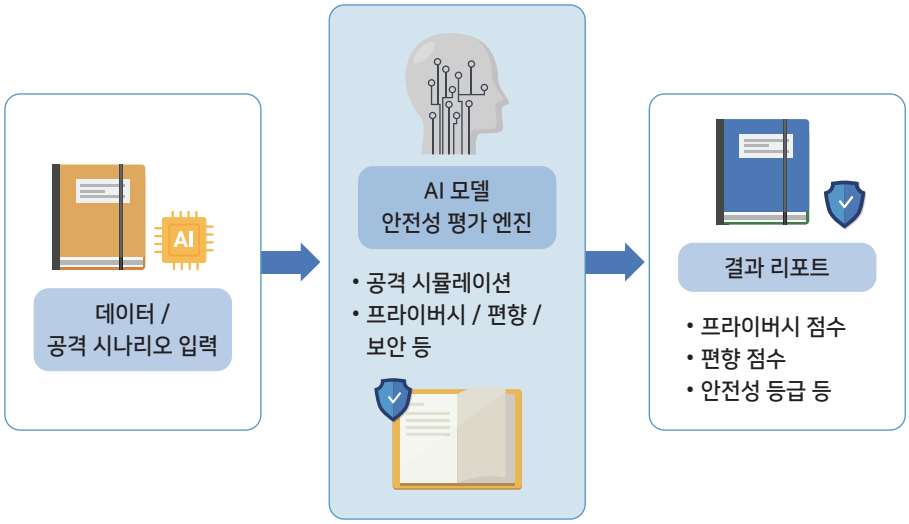
표준화 추진

- [국제표준] 마이데이터 서비스의 권리·통제 지원 요구사항 정립
  - DID·SSI 지갑을 활용한 '동의 관리, 열람·정정·삭제·이동 요구권 등'에 대한 안전한 처리 및 정합성 검증 절차 표준
  - 마이데이터 서비스 관련 디지털 지갑과 서비스 간 연계를 위한 기본 인터페이스·보안·프라이버시 요구사항을 국제표준으로 제안

- [국내표준] 국내 기준·연계 규격 정비를 통해 국제표준으로 연계
  - 산업 분야 간 마이데이터 전송 절차, 표준 API 규격·명세 등의 정합성을 확보하고, 디지털 지갑-서비스 연계에 필요한 API 표준모델 구체화
  - 국내 유관표준*을 참조하여 전송요구 관련 검증가능한 자격증명(VC) 규격, 송·수신 절차 등 통제에 필요한 상호운용 체계를 국제표준으로 연계

* 검증가능한 크리덴셜 발급/제출을 위한 메시지 포맷 및 전달절차(TTAK.KO-10.1560)

8. AI 모델 안전성 평가



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
AI 모델 안전성 평가	파운데이션 모델 학습데이터의 프라이버시 리스크 관리 기술				
	파운데이션 모델 운용 과정에서 민감정보 추론 방지 기술				
	생성형 AI 모델의 프라이버시 취약성 평가 및 개인정보 생성 억제(성능 저하 최소화) 기술				
		선택적 언러닝 및 검증 가능한 모델에서의 개인정보 삭제·파기 기술 개발			
			[국제표준] 파운데이션 모델 학습데이터 프라이버시 리스크 평가·완화 가이드라인 및 요구사항 국제표준		
			[국제표준] 개인정보·편향·보안을 포함한 AI 모델 안전성 평가 지표·벤치마크 및 시험방법 국제표준		

기술 세부내용

- 파운데이션 모델(Foundation Model) 학습데이터의 프라이버시 리스크 관리 기술
  - 학습데이터 구성·수집 경로·민감정보 비율 등을 분석
  - 재식별·누설 가능성을 점수화하고, 제거·마스킹·대체 전략 수립

- 파운데이션 모델 운용 과정에서 민감정보 추론 방지 기술
  - 멤버십·속성추론·인버전 공격 시나리오에 대한 모의공격·모니터링
  - 출력 필터링·로그 분석·경계 모델 등으로 민감정보 노출 차단

- 생성형 AI 모델의 프라이버시 취약성 평가 및 개인정보 생성 억제(성능 저하 최소화) 기술
  - 프롬프트 기반 개인정보 생성 여부를 테스트하는 평가 시나리오 구성
  - 개인정보 생성 가능 구간만 선택적으로 억제하면서 모델 성능 저하를 최소화하는 제어 기법 개발

- 선택적 언러닝 및 검증 가능한 모델에서의 개인정보 삭제·파기 기술
  - 특정 사용자·데이터를 활용한 부분 언러닝(unlearning) 알고리즘 설계
  - 언러닝 적용 후, 영향 범위·효과를 계량화하고 삭제·파기 증명* 형태로 제공

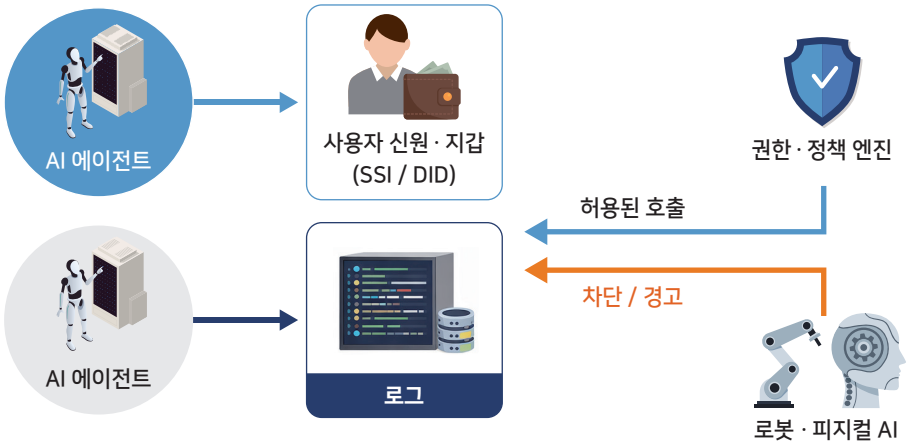
  * (예시) 변조방지 증적(감사로그) 기술, 삭제 증명 토큰 발급 기술, 삭제 후 재학습한 모델과 언러닝 적용 모델 간 유사성 비교·확인 기술, 언러닝 효과 시험·검증 기술 등

표준화 추진

- [국제표준] 파운데이션 모델 학습데이터 프라이버시 리스크 평가·완화 가이드라인
  - 학습데이터 수집·정제·라벨링 단계별 프라이버시 리스크 요소 정의
  - 리스크 평가 절차와 완화(제거·마스킹·합성 익명화 등) 요구사항을 글로벌 수준의 통용 가능한 지침으로 규격화

- [국제표준] AI 모델 안전성 평가 지표·벤치마크 및 시험방법 정의
  - 개인정보 노출, 편향, 보안 취약성 등의 관점에서 범용성 높은 지표를 제작
  - 시험용 데이터 집합, 평가 시나리오, 비교평가 기준(벤치마크)을 국제 수준으로 표준화하여 모델 인증·비교평가에 활용 가능하도록 제안

9. 에이전트·도구·로봇 실행 보안



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
에이전트·도구·로봇 실행 보안		에이전틱 AI 기반 개인정보 전 생애주기 자동 거버넌스 및 위험 예측·보호조치 기술			
		멀티모달 맥락 인식 기반 개인용 프라이버시 코파일럿: 트랜스포머·AI 에이전트를 활용한 다채널 개인정보 유출 점검·상담 자동화 기술			
		PET 조합 기반 Agentic/Physical AI 행동정책 설계·검증 및 프라이버시 보존 실행엔진 기술			
			에이전트 계정·지갑(SSI·DID 등)과 연계된 사용자 신원·권한·동의 관리를 통한 안전한 실행 통제 기술		
		[국제표준] AI 에이전트 권한·정책 언어 및 정책 집행·신원 연계 인터페이스 국제표준			
		[국내표준] 에이전트-도구/플러그인 연계 시 보안·프라이버시 요구사항 및 권한·동의 위임 모델 국내 표준			

기술 세부내용

- 에이전틱 AI 기반 개인정보 전 생애주기 자동 거버넌스 및 위험예측·보호조치 기술
  - 에이전트를 통한 수집-이용-보관-제공-삭제 등 전 과정 모니터링
  - 위험 징후 예측 및 자동 마스킹·차단, 추가 인증 등 보호조치 수행

- 개인용 프라이버시 코파일럿: 다채널 개인정보 유출 점검·상담 자동화 기술
  - 이메일, 메신저, 클라우드, SNS 등 여러 채널을 에이전트가 점검
  - 의심 유출·과다 공유 현황을 정보주체에게 자동 안내하고, 설정 변경·삭제·문의 등을 지원하는 상시적인 위험 관리·대응 기능 개발

- PET 조합 기반 에이전틱·피지컬 AI 행동정책 설계·검증 및 실행엔진 기술
  - 휴머노이드 로봇 등 피지컬 AI에 대하여 동형암호, 차분 프라이버시, 가명처리 등 PET을 조합한 행동정책(Rule Set) 정의 및 설계
  - 에이전트·로봇의 행동이 개인정보 보호 관련 정책의 위반 여부를 사전 검증하고, 실행 단계에서 정책 준수를 의무화하는 엔진 구현

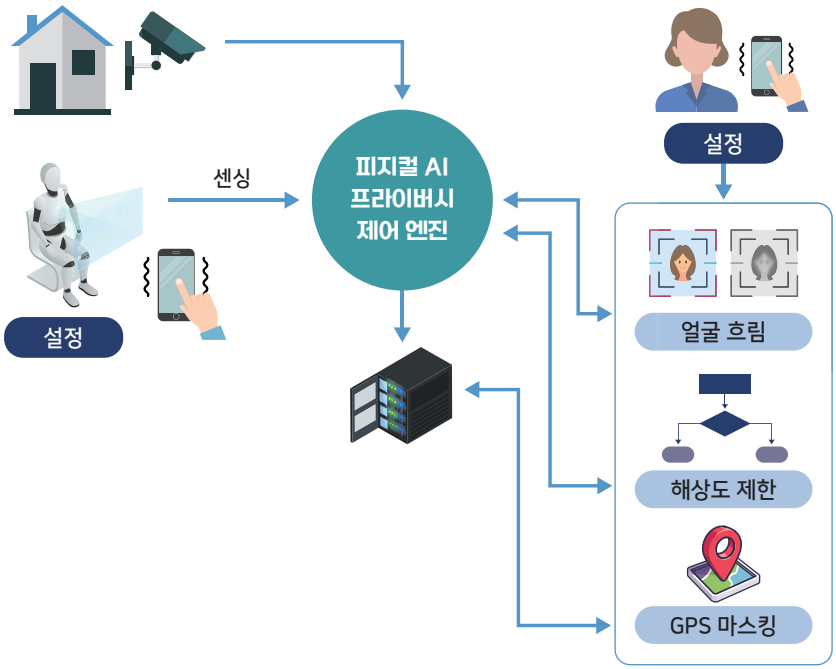
- 에이전트 계정·지갑(SSI, DID 등) 연계 신원·권한·동의 관리 기반 실행 통제 기술
  - 에이전트가 사용하는 계정·지갑을 사용자 DID·SSI와 연계
  - 자동화된 환경 하에서 사용자 신원·역할·동의 범위에 따라 도구·API 호출 권한과 실행 범위를 제한

표준화 추진

- [국제표준] AI 에이전트 권한·정책 언어 및 정책 집행·신원 연계 인터페이스
  - 에이전트의 접근권한 도구·API 연계활용 등을 위한 조건 등을 정의하는 정책 언어·모델 정의
  - DID·SSI 기반의 신원과 연동되는 정책집행 및 인터페이스 구조를 국제 표준으로 추진

- [국내표준] 에이전트와 도구/플러그인 간 연계시 보안·프라이버시 요구사항 및 권한·동의 위임 모델 표준화
  - 에이전트가 외부 도구·플러그인 호출 시 필요한 인증·인가·로깅·동의 관리 등에 필요한 기술적 요구사항 정의
  - 에이전트 활용 시에 사용자 권한·동의 위임 범위·방식, 위임 모델·API에 대한 규격을 표준으로 추진

10. 피지컬 AI 실시간 프라이버시 제어



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
피지컬 AI 실시간 프라이버시 제어		피지컬 AI·로봇 융합 환경을 위한 프라이버시 인지형 신원·행동 관리 및 최소수집 기술			
			로봇·IoT 등 실환경에서 개인정보 안전교환 프로토콜 및 상호작용 기술		
			[국제표준] 로봇·IoT·스마트기기의 센싱·저장·전송 단계별 프라이버시 보호 설계·운영 가이드라인 국제표준		
			[국내표준] 피지컬 AI 서비스에 대한 프라이버시 영향평가(PIA)·위험등급 분류 및 인증 기준 국내표준		

기술 세부내용

- 프라이버시 인지형 신원·행동 관리 및 최소수집 기술
  - 휴머노이드 로봇 등 신종 로봇 및 피지컬 AI가 사람·공간 인식하기 위한 필요 최소범위(시야, 해상도, 저장 시간)만 수집하도록 제어하는 기술
  - 정보주체의 식별정보와 행동에 대하여 본연의 역할 및 상황 별로 인지하고 제한 또는 비식별화하는 정책·엔진 개발

- 로봇·IoT 실환경에서 개인정보 안전교환 프로토콜 및 상호작용 기술
  - 로봇·센서·IoT 등의 장치와 사람 간 상호작용에 필요한 개인정보 송·수신 조건을 정의
  - 개인정보 등 데이터 전송 과정에 암호화·인증·무결성 보장을 포함한 안전한 통신 프로토콜 설계 및 구현

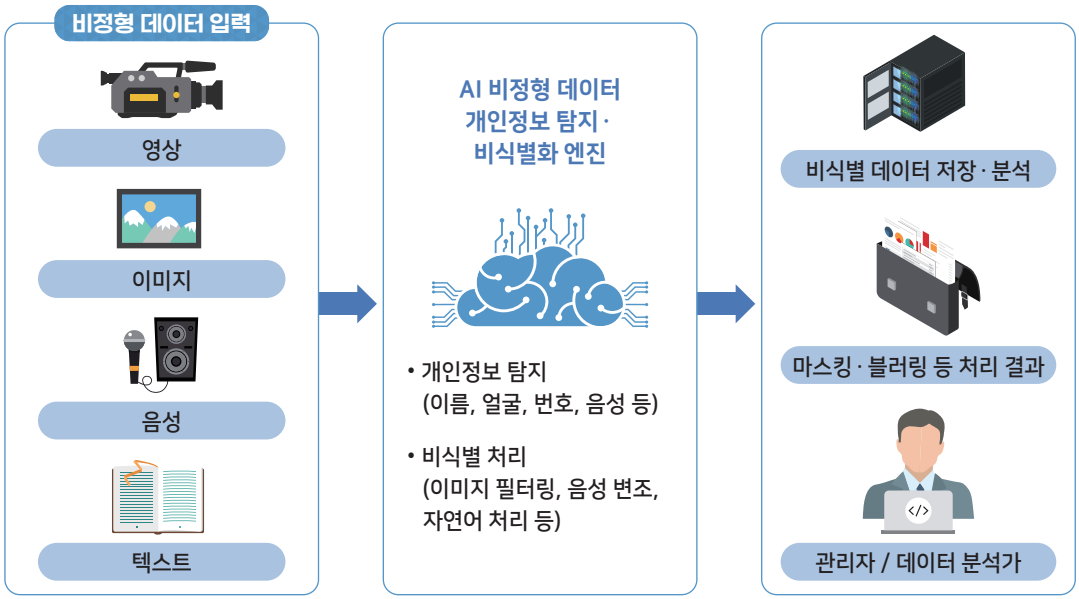
표준화 추진

- [국제표준] 로봇·IoT·스마트기기 프라이버시 보호 설계·운영 가이드라인
  - 각종 피지컬 AI 기기에서 구동되는 센싱-저장-전송 단계 별 '최소 수집, 보존기간, 접근통제, 로깅 등' 요구사항 정의
  - 서비스 설계·구현 및 운영 시, 국제적으로 통용될 수 있는 지침서 및 레퍼런스 아키텍처 제안

- [국내표준] 피지컬 AI 서비스에 대한 프라이버시 영향평가(PIA)·위험등급·인증 기준 표준 추진
  - 로봇·CCTV·생활 IoT 등 피지컬 AI 서비스의 'PIA 항목, 위험등급 분류 기준, 인증·적합성 평가' 등을 절차화하여 국내표준*으로 정립

  * 평가 방법론, 점검표(체크리스트), 결과보고 서식 등을 포함

11. AI기반 비정형데이터(영상, 텍스트, 음성 등) 비식별화



: 기술 / : 표준

핵심 기술	2026	2027	2028	2029	2030
AI기반 비정형데이터 (영상, 텍스트, 음성 등) 비식별화	멀티모달형 AI 기반 개인정보 탐지 추적 및 비식별화 기술				
			트랜스포머 기반 텍스트 개인정보 탐지 및 한국어·다국어 개인정보 탐지용 파운데이션 모델·오픈소스 라이브러리 개발 기술		
			[국제표준] AI 기반 비정형데이터 개인정보 탐지·비식별화 성능 평가용 벤치마크·지표·시험방법 국제표준		
			[국내표준] 로그·대화·비정형데이터 개인정보 탐지·비식별 결과 공통 포맷·연계 인터페이스 국내 표준		

기술 세부내용

- 멀티모달형 AI 기반 개인정보 탐지·추적 및 비식별화 기술
  - '영상, 이미지, 음성, 텍스트 등'에서 개인정보 탐지 및 '얼굴, 음성 특징 등' 민감정보를 인식하는 기술
  - 탐지된 개인정보는 마스킹, 대체, 변조 등 비식별 처리하고, 재식별의 위험도를 낮추는 기술 개발

- 트랜스포머 기반 텍스트 개인정보 탐지 및 한국어·다국어 파운데이션 모델·라이브러리 개발
  - 이메일·채팅·문서 등 텍스트에서 이름·주소·계좌 등을 자동 식별하는 문맥 기반의 기술 개발
  - 한국어·다국어를 지원하는 개인정보 탐지용 파운데이션 모델 및 오픈소스 라이브러리 구현

표준화 추진

- [국제표준] 비정형데이터 개인정보 탐지·비식별화 성능 평가 비교평가 기준·지표·시험방법
  - 텍스트·영상·음성 등 매체별 탐지 정확도, 비식별화 품질, 재식별 위험도 등을 평가하는 공통 지표로 정의
  - 시험용 데이터·평가 시나리오·시험 절차를 국제 공통 비교평가 기준으로 표준화

- [국내표준] 로그·대화·비정형데이터 개인정보 탐지·비식별 결과 공통 포맷·연계 인터페이스
  - 개인정보처리 시스템 내 각종 로그·대화기록·멀티미디어 파일에서 탐지·마스킹·비식별 처리 과정·결과에 대한 저장관리 방안 정의
  - 개인정보 탐지·비식별화 결과(로그, 메타데이터 등)를 사전예방 목적으로 유관기관·서비스 간 공유·연계 가능한 API 통신체계 및 규격 표준화

2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵

Ⅶ 기대효과

CHAPTER
VII 기대효과

AI·데이터 경제 확산에 대응한 선제적 개인정보 보호·활용 기술 확보

- 에이전틱 AI 등 신기술 환경에서 개인정보의 안전 활용을 보장하는 전주기 보호·활용 기술(PET 스택)을 지속적으로 확보 및 운용 가능
- 국내 「개인정보 보호법」, GDPR, EU AI Act 및 각종 AI 관련 법·가이드라인이 요구하는 프라이버시·책임성·투명성 요건을 충족하는 기술을 고도화
- 글로벌 빅테크의 프라이버시 내재화 전략에 대응하여, 동형암호·차분 프라이버시 등 핵심 PET·AI 융합 기술의 국내 경쟁력 확보
- 안전한 활용 기술 수요와 정보주체 권리보장 기술 수요에 대응하여 개인정보 보호·활용 특화 신시장 창출

신뢰 기반 디지털·AI 사회 구현에 기여

- AI와 관련한 다양한 신기술에서의 대규모 데이터 활용 시 개인정보 오·남용, 재식별, 프롬프트 공격 등 AI 특유 위험에 대한 우려 해소
- 데이터·AI 경제에서의 고부가가치 서비스 및 신산업 창출을 지원하고, 국민이 안심하고 서비스를 이용할 수 있는 신뢰 기반 디지털 사회 조성

개인정보 보호와 안전한 활용 정책을 뒷받침하는 인프라 구축

- 「개인정보 보호법」 및 관련 정책에서 요구하는 가명·비식별 등 안전활용 정책을 기술적으로 구현할 수 있는 표준 인프라 구축
- 국내·국제 규범 및 표준과 정합성을 유지하는 R&D·표준화·인력양성 체계를 마련함으로써, 지속 가능한 개인정보 보호·활용 생태계를 지원

주요 핵심기술(11개) 개발 및 표준화 완료 시, 기대효과

연번	핵심기술	R&D 산출물 (응용기술/서비스 형태)	표준화 산출물 (국제/국내)	기대효과 (사회·산업 변화 중심)
1	정책 준수 증명 결과 열람 + 보존형 검색증강생성 (RAG)·삭제증명 (설계기반 삭제, Forget-by -Design)	· 컴플라이언스 준수 증명 플랫폼·모듈 - 열람·정정·삭제·이동 등 권리행사 실행과 삭제 완료 증명용 토큰·로깅 기술	(국제) 프라이버시 중심 설계(PbD) 기반 권리보장·증명 요구사항 및 참조 모델 (국내) 동의·처리·권리행사·삭제 이력 공통 데이터관리 형식 및 인터페이스 표준모델	· 공공을 넘어 민간으로 확산되는 AI 서비스 신뢰 기반 형성 - 삭제 등 요청 시 신뢰기반 증명을 통해 정보주체의 권리보장 실효성 증대(분쟁 등 비용감소)
2	딥페이크/합성 검증·레이블링	· 사전예방형 변환기술 (워터마크/노이즈 등) - 진위검사 결과 표시 및 경고·차단 기술과 연계	(국제) 진위검사 결과 공통 메타데이터·화면표시 방식 (국내) 유관기관 간 결과 공유 인터페이스·프로토콜	· 통일된 안전표시 및 공유체계로 전환 - 허위콘텐츠·보이스피싱 피해 사전예방·대응 속도 개선
3	엣지 디바이스 개인정보보호	· 온디바이스 격리 환경에서 이상행위 탐지 즉시 자동 통제(격리/차단/추가 인증/경고)	(국제) 엣지·모바일 개인정보보호 아키텍처·접근통제 요구사항 (국내) 탐지·차단 기능 및 로그관리 시험·평가기준	· 장치(단말)에서 유출위험을 조기 차단하는 기술이 현실화되어 실시간 예방체계로 가동 - 국내·외 표준화와 연계로 엣지 디바이스 공공 단말 보안 기준·조달요건에 반영 가능
4	다크웹·표면웹 유출 탐지 (공개출처정보 (OSINT))	· 불법유통 패턴 분석·공급망 위험지수 산출 - 노출된 자산 스캐닝·취약점 식별 및 성능평가 기술 등	(국제) 공개출처정보(OSINT) 수집·교환 포맷 및 기관 간 인터페이스 (국내) 유출 탐지·분류·신고 공통 데이터 모델·API	· 공급망 위험지수 기반의 사전 위험 경보로 전환 - 경보-조치-재발방지로 이어지는 선순환 체계(유관기관과 합동 대응체계 가동)
5	재식별 위험도 평가·검증	· 공격유형·절차·위험도 산정 - 안전성 등급·검증·보고서 표준 템플릿 적용	(국제) 재식별 위험도 평가 방법론·지표 (KS) (국내) 안전성 등급·검증절차 등	· 가명·비식별의 정량화 및 등급화된 환경의 안전한 의사결정 지원 기술로 활용 - 공공데이터 등에서 개방·결합을 통한 안전한 활용 체계 확산
6	합성데이터 등 PET 기반 비식별화 (단일·하이브리드)	· 보유기간 제한을 고려한 시계열 합성데이터 생성 기술 - 품질·유용성·재식별위험 등을 검증 병행	(국제) 합성데이터 품질·프라이버시·유용성 평가 및 시험방법 (국내) PET(합성·차분 프라이버시·가명처리 등) 연계 프로파일 및 참조 모델	· 익명화된 분석·학습용 데이터 공급 확대 및 활성화 - 공공·금융·의료 등 다양한 산업 분야에서 실증 및 활용사례 축적

연번	핵심기술	R&D 산출물 (응용기술/서비스 형태)	표준화 산출물 (국제/국내)	기대효과 (사회·산업 변화 중심)
7	마이데이터 동의·위임 통합 자동화 플랫폼 (SSI/DID)	· 자기주권신원(SSI) 기반 개인정보 지갑 레퍼런스 (발급·저장·제출·철회) - 공공 등 마이데이터 서비스 연계 및 보안 검증	(국제) 정보주체 권리·통제권 보장 요구사항(지갑-서비스 연계 인터 페이스/보안/프라이버시) (국내)	· 정보주체의 지갑을 통한 동의·철회·이동권 지원 편의성 강화 - 웹·앱 등에 흩어져있는 개인정보를 정보주체가 직접 관리할 수 있는 환경으로 정착
8	AI 모델 안전성 평가	· 학습데이터 프라이버시 리스크 관리 기술 - 민감정보 추론 방지 및 프라이버시 취약성 평가·제어 기술과 연계(선택적 언러닝 검증 포함)	(국제) 파운데이션 모델 학습데이터 프라이버시 리스크 평가·완화 요구사항 (국내) 개인정보·편향·보안 포함 안전성 지표·벤치마크· 시험방법	· 공공분야 AI 도입시 책임성·투명성 강화 - 평가, 검증 절차가 필요한 업무에서 안전성의 기준 정립
9	에이전트·도구·로봇 실행 보안	· 도구(Tools)·API 호출 시 인증·인가·로깅·동의위임, 정책언어·모델 정의	(국제) 탈중앙식별자(DID)/자기주권신원(SSI) 연동 정책집행·인터페이스 구조 (국내) 에이전트-도구/플러그인 보안·프라이버시 요구사항 및 권한·동의 위임 모델	· 개인정보 침해 리스크를 표준 기반 통제로 완화 - 불법적인 실행, 과다한 권한 등이 제한되어 산업에서 안전한 실행환경을 보장
10	피지컬 AI 실시간 프라이버시 제어	· 로봇·IoT 센싱/저장/전송 단계별 최소수집·행동관리 기술 - 안전한 개인정보 교환 프로토콜 등 정의 병행	(국제) 로봇·IoT·스마트기기 단계별 프라이버시 설계·운영 가이드 (국내) 피지컬 AI PIA·위험등급·인증 기준	· 미래산업 확산을 대비한 최적화된 설계·인증 체계를 선제 구축 - 스마트 도시, 제조, 돌봄 등 각 산업에서 신뢰가능한 AI로 활용 가능
11	AI 기반 비정형데이터 비식별화 (영상·텍스트·음성)	· 멀티모달 탐지·추적·비식별 - 한국어·다국어 탐지용 파운데이션 모델·오픈소스 환경의 기술 적용	(국제) 성능평가 벤치마크·지표·시험방법 (국내) 로그·대화·비정형 비식별 결과 공통 포맷·연계 인터페이스	· 안전성 검증체계 정착을 통해 실시간 활용 기술로 정착가능 - 의료, 치안, 공공 등 안전성 및 시급성 높은 분야 부터 기술 적용이 가속

※ (목표) 수요기반 R&D 수행 → 실증(공공) → 표준(국제/국내) → 시험·인증/조달 → 민간 확산으로의 선순환 체계 확립

별첨

2026 ~ 2035

개인정보 분야 전문인력 양성 로드맵

개인정보보호위원회
Personal Information Protection Commission

2026 ~ 2035

개인정보 분야
전문인력 양성 로드맵

목 차

Ⅰ 추진배경

AI 시대, 개인정보는 **AI의 성패를** 좌우하는 **핵심요소이자 취약점**

- AI는 방대한 양의 데이터를 학습·분석하여 작동하는데, 데이터 내에는 민감한 개인정보가 포함될 수 있어 **개인정보를 보호**하면서 **AI 개발에 활용**하는 능력이 핵심 성공 요인으로 부각

- 반면, AI 개발·이용에 **불투명한 개인정보 처리**는 법적 리스크를 유발할 뿐만 아니라 **이용자의 신뢰**를 잃어 시장에서 퇴출될 가능성

※ 딥시크 서버에 이용자 정보가 저장돼 데이터 악용 우려 제기, 미 해군 국방부, 하원이 딥시크 접속 금지, 일본 대만 등 각국 정부에서 공공부문 중심으로 딥시크 사용 금지 등(매경, '25.3.7.)

복잡·다양하게 진화하는 AI의 특성에 맞추어 개인정보 활용의 **「안전밸브」**역할을 수행할 **고급 인력 양성**이 필요

- 최근 AI는 더 다양한 매개변수를 활용하는 복잡한 구조로 발전하는 동시에 **커넥티드카 탑재, 피지컬 AI** 등 전 산업 영역으로 확대

- AI가 **복잡·다양화** 될수록 **개인정보 침해의 범위와 심각성**은 더욱 커질 가능성이 증가하여 **고급 인력 수요**가 급증 예상

전 세계는 **안전하게 개인정보를 AI에 활용**하는 것이 **글로벌 AI 경쟁력**의 원천임을 인식하고 **개인정보 인력 양성**에 집중 투자

- 미국 유럽 등 다수의 선진국은 **PET**(Privacy Enhancing Technology) **개발, 산업 및 표준 선점**을 위하여 전문인력 양성에 사활

- 그러나 우리는 학부 수준의 **기초 인력** 및 재직자 교육에 불과하여 우수한 인력이 기술개발을 선도하는 **선순환 생태계**는 아직 요원

- 개인정보 문제는 **기술·법제·경영** 등 **다각도의 접근·대응**이 필요한 분야임을 고려하여 정부주도의 **다학제적 융합 인재** 양성이 절실

국내에서는 '25년 **SKT 고객정보 유출 사고**(4월), **쿠팡 고객정보 유출사고**(11월) 등 전 국민에게 영향을 끼친 대규모 사건 다수 발생

- 특히, 국민의 실생활과 밀접한 **휴대전화, 온라인 쇼핑 등에 포함된 개인정보**가 무단 접속·**유출**되면서 **2차 피해**로 확산될 위험성 마저 존재

  ※ (SKT 유출 정보) 고객식별에 활용되는 USIM 정보 등 약 9.82GB 분량(쿠팡 유출 정보) 성명, 배송지 주소, 전화번호 등 약 34백만건의 이용자 정보

- 이로 인해, 다수의 국민이 이용하는 서비스에서 **유출 사고 발생 시** 직접적 피해 우려 외에도 **국민불편 초래** 등 **사회적 비용 심각**

  ※ (SKT) 3년간 7조원 손실 위기, 매출전망 8천억원 하향 조정('25.7.4. 연합뉴스)(쿠팡) 쿠팡 시총 13조원 날라갔다.. "주주소송 본격화"('25.12.11. 디지털타임스)

AI **기술 발전**으로 인해 예측 불가능한 형태로 유출 **보안 위협이 진화**하고, 개인정보 처리 **자동화·집중화**로 인한 **개인정보 유출위험은 지속 증가** 전망

※ 한국 기업 83%가 최근 1년간 AI 관련 보안사고 경험('25년 사이버보안 준비 지수, CISCO)

- 특히, 산업 전 분야에 걸쳐 AI 활용이 급속히 확산되면서, 새로운 유형의 유출사고가 등장하고, 사건은 점차 **대형화·복잡화**

- 국내 다수 기업은 **AI 심화 시대**에 맞는 성숙한 **개인정보 리스크 관리 체계**를 갖추지 못하고 있어, 국내 대규모 사고 **재발 우려 심각**

  ※ 한국 기업 사이버보안 '성숙' 단계 3%, 사이버위협으로 비즈니스 차질 예상 46%(CISCO)

개인정보 보호·활용 기술 **연구개발**을 **국제적인 수준**으로 **선도**하고, **산업현장**에서 사전 예방, 사후 대응 등 **개인정보 처리 전반**에 걸쳐 **안전하게 활용**할 수 있도록 특화된 **전문인력 양성** 추진 필요

Ⅱ 국내·외 추진현황

국내 교육기관(대학)의 인력양성

- **정보보호 대학원 내 특수대학원** 형태로 인력 양성(2개교), **학부과정** 마이크로디그리(MD), 부·복수·융합전공 운영('26.上 기준)

  - 주요 대학에서 **개인정보 보호 대학원**('24.9.~) 및 **개인정보 보호 트랙**('22.9~)을 운영 중

- **교육부「혁신인재양성사업」**으로 개인정보 관련 **학부**과정* 운영('25.2. 종료)

  * 강원권(주전공, 마이크로디그리), 서울권(마이크로디그리, 부 복수전공 및 융합전공)

[참고] 개인정보 보호 분야 혁신인재양성사업

- (목적) 산업·경제 구조 변화에 대응한 혁신인재 양성을 위해 개인정보 보호 분야 대학 특성화 지원('24년 25억원)
- (주관) 개인정보보호위원회
- (기간) '22.3.~'25.2.(3년)
- (대상) 국내 4년제 대학 중 총 5개교
- (내용) 전공개설, 교과개발, 글로벌 인재양성, 실습환경 및 인프라 구축, 산학협력 및 취·창업 역량 강화

국외 교육기관(대학)의 인력양성

- 미국, 네덜란드 등에서 개인정보(privacy) 석사과정 운영 중

  - 미국 카네기 멜론 대학교는 개인정보 보호 공학(Privacy Engineering) 석사 프로그램 운영('13~)

- (목적) 개인정보 보호 엔지니어 또는 기술적 개인정보 관리자 역할을 준비하며, 개인정보 보호 설계(Privacy-by-Design) 원칙을 제품 및 서비스에 통합하는 능력을 배양
- (주요 커리큘럼) 5개 핵심과정*(66개 필수과목, 42개 선택과목 등으로 구성) 및 개인정보보호 중심 설계(PbD) 실습, 캡스톤 프로젝트 등 실무 프로젝트 운영

* Information Security, Privacy, and Policy(17-631), Foundations of Privacy(17-731) 등

  - 미국 텍사스 대학교 오스틴은 정보보안 및 개인정보 보호 과학 석사 프로그램(MS SIP, Master of Science in Information Security and Privacy) 운영

- 사회, 공공 정책 등의 정보보안 및 개인정보 보호에 관한 10개 과목으로 교육과정 운영

※ Information Security & Privacy in Society(ISP 381), Public Policy, Information Security, and Privacy(ISP 382) 등

- 네덜란드 마스트리히트 대학교는 개인정보 보호, 사이버 보안, 데이터 관리와 관련된 전문 석사 프로그램(Advanced Master in Privacy, Cybersecurity and Data Management) 운영

- GDPR 및 국제 데이터 보호 규정, 개인정보 보호와 사이버 보안의 법적·기술적 측면 등의 주제로 교육과정 운영

※ European Privacy and Data Protection Fundamentals(LAW5072), Advanced Privacy and Data Protection Law(LAW5076) 등

국내·외 유관분야 대학원 연구지원 사업 현황

- ITRC(대학ICT연구센터 사업, Information Technology Research Center)
  - **(목적)** AI, 6G, 반도체, 양자통신 등 미래 ICT 핵심기술 연구 지원, 석·박사급 ICT 고급 연구인력 양성 및 산학협력 활성화
  - **(대상)** ICT 분야 특성화 대학(연구센터 단위)

※ 전국 약 40개 대학, 60여 개 연구센터 운영(2025년, 64개 센터, 542억여원 지원)

  - **(내용)** 센터 내 석·박사/통합과정 학생에게 연구장학금, 인건비, 국제학회, 산학프로젝트 비용 등 지원

※ 센터 단위로 중장기(보통 6~8년 내외) 과제 지원

- '연구 + 교육 + 산학 + 창업'이 연계되어 연구센터를 지원하는 방식

※ 기업과 공동연구, 인턴십, 현장실습, 기술이전, 창업 연계까지 한 패키지 안에서 운영

- BK21(4단계 두뇌한국21(BK21 FOUR) 사업)
  - **(목적)** 세계적 수준의 연구중심대학 육성, 대학원 연구역량 제고 및 안정적인 연구비 지원

※ 이·공계 외에도 인문사회, 예체능, 기초과학 포함 전 학문 분야를 포함

  - **(대상)** 교육연구단·팀 소속 대학원 석·박사 과정(통합과정 포함) 등

※ 4단계 BK21(2020~2027) 기준, 연간 지원예산 약 5,225억 원

※ 참여대학 63개, 교육연구단(팀) 587개 운영(미래인재·혁신인재·대학원혁신 지원 등)

  - **(내용)** 연구장학금, 해외연수·국제학술대회 참가, 외국어 및 연구역량 강화 프로그램 등 지원

- 전 학문분야 대상 전국 규모 기본 인프라 사업

※ 대학원 재학생을 대상으로 연구비·생활비를 포괄하여 지원하는 대표적인 사업

• 해외 연구지원 프로그램

국가	과정명	내용
미국	NSF - GRFP (Graduate Research Fellowship Program	· **(주관)** 미국 국립과학재단(NSF) · **(대상)** 미국 내 대학에서 STEM/교육 분야 연구기반 석·박사 과정을 수행하는 대학원생 · **(내용)** 3년간 연간 생활비(Stipend) + 대학에 지급되는 학비 지원(Cost-of-education allowance) 패키지 ※ 미국 내 대표적인 국가급 대학원 연구장학 프로그램
EU	MSCA	· **(주관)** 유럽연합(EU) Horizon Europe 프로그램 · **(대상)** 네트워크에 선발된 박사과정 후보자 · **(대상)** 급여 수준의 연구자 급여 + 이동·가족수당 등 공동 학위 또는 이중학위, 산학 연계 연구, 산업체 Secondment 기회 제공 ※ "연구 + 국제이동 + 산학협력 + 공동학위"를 통합한 유럽형 박사 인재양성 플래그십
싱가포르	A*STAR Graduate Scholarship (AGS)	· **(주관)** 싱가포르 과학기술연구청(A*STAR) · **(대상)** 싱가포르 국립대(NUS, NTU 등) 또는 A*STAR 산하 연구소에서 이공계·ICT·데이터·AI 분야 박사과정을 수행하는 국내·외 우수 인재 · **(대상)** 박사과정 전 기간 등록금 전액 지원, 월 생활비(급여형 장학금) 지급, 연구비 및 학회 참가비, 해외연수 기회 제공 ※ "연구자 고용형 박사 장학 + 국가 R&D 인력 파이프라인" 구조
일본	JSPS Fellowships	· **(주관)** 일본학술진흥회(JSPS) · **(대상)** 일본 내 대학에서 박사과정(또는 박사과정 진학 예정)인 연구자 등 · **(대상)** 개인 단위 펠로우십, 월 연구장려금(생활비 성격) + 연구비 별도 지원, 지도교수 연구과제와 독립적으로 개인 연구 수행 ※ 학생이 아닌, 독립 연구자로서의 박사·박사후 과정 지원

• 연구지원 방식 비교(국내 - ITRC, BK21, 해외 - 연구지원 프로그램)

구분	ITRC	BK21	해외
주관 부처	과학기술정보통신부 / IITP	교육부 / 한국연구재단(NRF)	미국 NSF, EU(EC), UKRI, DFG, JSPS 등
사업 목적	ICT 핵심기술 연구 강화 및 석·박사급 고급 인재 양성	세계수준 연구중심대학 육성 및 학문후속세대 양성	글로벌 우수 연구인력 양성 및 국제 연구경쟁력 강화
지원 단위	대학 내 연구센터 단위	대학 내 교육연구단(팀) 단위	개인 단위 펠로우십 또는 국제 컨소시엄/네트워크 단위
지원 대상	ICT 분야 연구센터 소속 석·박사 및 통합과정생	전 학문 분야 BK21 참여 대학원 석·박사 및 통합과정생	석·박사 과정생 및 박사 후 과정(Post Doc.) 연구자(국가·프로그램별 상이)
지원 분야	AI, 데이터, 보안, 반도체, 6G 등 ICT 특화 분야	이공계 + 인문사회 + 예체능 등 전 학문 분야	STEM 중심이나 인문·사회 포함 (프로그램별 상이)
지원 내용	연구인건비, 장학금, 국제학회 참가, 산학프로젝트 참여	연구장학금(생활비), 해외연수, 연구역량 강화 프로그램	생활비(Stipend), 등록금, 연구비, 이동·가족수당 등
수행 방식	교수·기업 참여 센터 중심 공동연구	교육·연구 병행 연구단 중심 운영	학생 중심 독립 연구 또는 국제 공동연구
요 약	**분야특화·센터 중심 고급인재 양성**	**국가 차원의 대학원 기본 인프라 사업**	**개인 또는 국제 네트워크 중심 글로벌 인재양성**

Ⅲ 시사점 및 전문인력 양성 방향

전 세계적으로 **AI 신뢰성, 데이터 안보**에 대한 정부 지원 가속화, 동시에 **프라이버시가 주요 이슈**로 부상*하며 **프라이버시 리스크 대응 기술 개발** 및 **국제공동연구** 등이 가능한 **전문가 양성 필요**

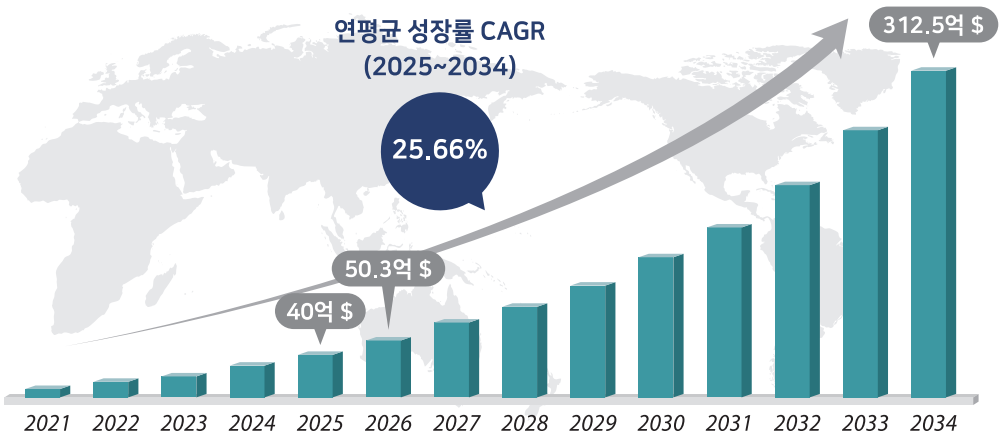
* 美 NIST 주도 개인정보보호와 AI 신뢰성을 위한 기술 표준화 강화 발표('24, AI RMF), EU 디지털유럽 프로그램에서 AI와 개인정보보호 기술 표준화를 추진하며 예산 증액('24, KERC)日 1,180억 엔 투자 초거대 데이터 환경에서의 AI 개발-활용-리스크 대응('24, KOTRA)

- 개인정보 강화 기술(PET) 관련, 전 세계 시장은 **약 50억 달러**('26년, 한화로 약 7.5조원)에서 **약 312.5억 달러**('34년, 약 47조원)까지 **성장** 전망

  - AI-PET 결합, PbD 내재화, 데이터 활용 과정에서의 보호, 클라우드 등 IT 인프라 내 **PET 적용 확산에 따른 연구개발 수요**가 큰폭 증가할 것으로 예상

  - 개인정보 보호와 안전한 활용을 동시 충족하는데 핵심기술로 PET가 주목받고 있으며 현재 **북미지역이 가장 큰 시장 점유율**(약 36%) 차지*

* ① (전 세계 연평균성장률) 25.66%　② (시장점유율) 유럽: 29%, 아시아 태평양: 25%, 기타: 10% 등



※ 출처: Privacy Enhancing Technologies Market Size, 2021-2034(Fortune Business Insights, '26.3월)

- **과징금 처분 본격화***에 맞춰 개인정보 전문인력 확보를 통한 **법 위반행위 예방·대응 체계**로 전환하여 **제도 실효성 확보**

* A사 151억('24.5.), B협회 4.8억('24.9), C대학 1.8억('24.11), D·E·F 보험사 92억('24.12), G사 5억('25.1) 등, 중소기업·스타트업도 다수 포함

「개인정보 보호법」 전면 개정('24.3. 시행)으로 **규제가 현실화** 됨에 따라 **전문가 육성을 병행 지원**하여 **공공·민간의 대응력 향상** 필요

- 개인정보 **보호책임자(CPO)** 역할 강화, 자격요건 법정화('24.3.)*로 **급증한 전문인력 수요**를 교육 시장의 **자발적인 전공 개설 및 인력 배출**만으로 모두 **소화하기에는 무리****

* 개인정보 보호, 정보보호, 정보기술 경력 총합 4년 이상, 개인정보 보호 경력 최소 2년 이상 보유(개인정보보호 관련 박사 등 학위 취득으로 경력 인정 가능)

** '24년 기준 약 700여개 기관에서 CPO 법정 자격요건 충족 필요, 고려대, 서울여대 등 국내 개인정보 보호 대학원 및 학부 졸업생 규모는 '25.2 기준 50명/연 이내

대상	대상기관(공공·기업 등)	비고
대규모 개인정보처리자	약 600여개	· 연 매출액 1,500억원 이상 · 대규모 개인정보 처리자 ※ 100만명 이상 개인정보 또는 5만명 이상 고유·민감정보
대학교육기관	23개	· 재학생 2만 명 이상 대학교 ※ 대학원 재학생 수 포함(직전년도 12/31 기준)
상급종합병원	47개	· 「의료법」 제3조의4에 따른 상급종합병원
공공시스템운영기관	63개	· 개인정보위가 고시하는 기준*에 해당하는 개인정보처리시스템을 운영하는 공공기관 * 개인정보 처리 규모, 접근권한을 부여받은 개인정보 취급자의 수 등

지속 제기된 민간·공공기관 개인정보 전문인력 수요에 부응할 필요

- 특히 AI, 가명정보, 익명처리 등 **고도화된 기술력에 대한 이해**를 바탕으로 개인정보 처리, 사고예방 등이 가능한 **전문인력 수요 증가**

개인정보 보호 및 활용 조사('24)

- 개인정보 보호 시 애로사항
  - **담당 인력 전문성 부족**: 공공(62.2%), 민간(27.2%)
  - 개인정보 보호 관련 기술 부족: 공공(55.0%), 민간(27%)
- 우선되어야 할 정부 정책
  - 개인정보 **기술개발** 및 보급 촉진(공공 76.7%, 민간 25.2%)

개인정보 보호 및 활용 조사('25)

- 현장에서는 개인정보 분야 전문인력이 매우 부족(6,000여개 기업 대상 응답조사 결과)
  - 개인정보 보호책임자(CPO) 전담여부: 전담(6%), 정보보호책임자 겸직 및 기타업무(94%)
  - CPO 업무경력: 1년 미만(91.4%), 유관분야 학위 보유자(0.5%)
  - 개인정보 분야 전문인력 부족: CPO 이외 담당자 존재(5.3%), 담당부서 없음(51.4%)

  * 담당부서가 있는 경우에도 개인정보보호 전담부서가 있는 경우는 0.1%에 불과

사이버보안인력수급실태조사('24)

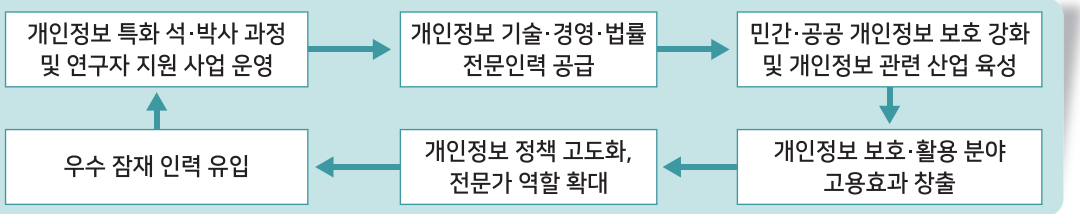
- **업종별 사이버보안 인력이 부족한 직무**(중복응답)
  - 전문·과학 및 기술 서비스업 압도적 1위(46.8%), 운수업 및 창고업 2위(44.8%)가 "**개인정보보호 관리·운영**"
- **업종별 사이버보안 인력 채용 계획**
  - 전문·과학 및 기술 서비스업 1위(사고분석·대응, 55.4%), 2위(**개인정보 보호**, 22.3%)

개인정보 보호 분야는 투자우선순위가 높은 사안이 아님에 따라 자생적 산업기반 및 생태계 구축을 기대하기 어려움

- 반면, **국민 권리와는 직결**되는 사안으로, **정부의 적극적인 지원**을 통해 **전문인력 양성을 포함한 생태계**를 조성·운영할 필요

- **형평성 차원**에서도 전문가 채용 및 전담인력 운영이 어려운 **중소기업·스타트업 애로해소**를 위해 정부 지원을 통한 **인력난 해소** 필요

개인정보 분야 전문인력 양성 생태계 구축



개인정보 분야 전문가 양성 비전 및 추진방향

비 전

개인정보 분야 전문인력 양성 및 연구자 지원으로 신뢰 기반 AI 시대 선도

추진전략

1	R&D 역량을 갖춘 핵심인재 양성	① 법·기술 마인드를 갖춘 융합형 인재양성 ② 개인정보 강화 기술(PET) 연구역량 확보 ③ 전문인력(CPO 등) 취업 연계 지원
2	산학연계 현장맞춤 인력 공급	④ 산업계 참여 교과과정 개발 ⑤ 이공계·실무경력 교원 확보, 통계 기반 구축 ⑥ 가명·익명 데이터 등 실습환경 구축
3	글로벌 AI 신뢰성 및 표준 선도	⑦ 해외 대학 연계 공동연구 수행 ⑧ AI 신뢰 증진을 위한 기술 표준 선점
4	미래선도형 연구자 양성	⑨ 차세대 개인정보 강화 핵심기술 분야 ⑩ AI 기반, 개인정보 보호 전주기 보호 기술 분야
5	신산업 대응 프라이버시 전문 연구자 양성	⑪ 개인정보 특화 유출사고 예방·조사 선도기술 분야 ⑫ 신산업 융합 개인정보 보호·활용 기술 분야

Ⅳ 중점 추진과제

【 1단계 - 전문인력 양성(석·박사급) 】

개인정보 분야 전문가 양성 로드맵(2026~2031, 총 640명 양성)

<table>
<tr><th>양성분야</th><th>지원대상</th><th>2026</th><th>2027</th><th>2028</th><th>2029</th><th>2030</th><th>2031</th></tr>
<tr><td rowspan="9">개인정보 분야
석·박사
전문인력 양성</td><td rowspan="5">보호·활용
전문가
2개교
(160명)</td><td colspan="2">개인정보 학과(전공) 및
차별화된 커리큘럼 개발</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2">개인정보 보호·활용 관련
신기술 연구·개발</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2">산·학 협력체계 구성</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="3">현장중심형 전문가, 기술 등 인프라 확보</td><td></td><td></td></tr>
<tr><td></td><td></td><td colspan="2">글로벌 역량 확보(해외 교육기관 협력 등)</td><td></td><td></td></tr>
<tr><td rowspan="4">예방·대응
전문가
6개교
(480명)</td><td></td><td colspan="2">개인정보 유출사고
예방·대응 커리큘럼 개발</td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td colspan="2">개인정보 사고조사
전용기술 연구·개발</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td colspan="2">AI 기반의 유출사고
예방·대응 실습환경 마련</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="2">산업계 취업 연계 지원</td></tr>
</table>

※ '27년 등 신규 예산확보 여건에 따라 추진시점과 양성 규모가 일부 변경가능

❶ 법·기술 마인드를 갖춘 융합형 인재양성

- **(컴플라이언스 역량)** 「개인정보 보호법」, 유럽 GDPR 등 국내외 **개인정보 관련 법제에 대한 심도 깊은 이해**를 통해 **컴플라이언스 관리**가 **가능**한 수준의 **개인정보보호책임자(CPO)급 인력 양성**

- **(다학제적 접근) 기술, 법률, 조직관리 및 경영** 각 분야 전문지식을 포함하여 개인정보 관련 **문제 상황의 예측 및 해결**이 가능한 인재 배출

- **(조사전문가)** 개인정보 유출사고 현장 초동대응 및 사후 심층 분석 등 **지역 특화형 행정조사 분야 전문역량 확보**를 위한 **석·박사급 인재 양성**

❷ 개인정보 강화 기술(Privacy Enhancing Technology) 연구역량 확보

- **(솔루션 개발)** 인공지능(AI) 확산, 급변하는 신기술 적용 환경에서 개인정보 침해에 대응 가능한 **분야별 상용화 솔루션 개발 과정 운영**

  ※ AI 파인튜닝 및 RAG 과정의 개인정보 유출 리스크 대응, AI 에이전트의 개인정보 차원 리스크 식별·대응 기술 등 개발

- **(원천기술 연구)** 동형암호, 차분프라이버시, 합성데이터 등 **PET에 대한 교육**을 바탕으로 **새로운 개인정보 원천·응용기술 연구 추진**

  ※ 개인정보 등의 데이터 처리흐름(수집·이용 등) 별 개인정보 보호 기술 연구

- **(사고분석 기술 연구)** 개인정보처리시스템의 개인정보 유출·침해 **사고 발생** 시, **신속하게 대응** 및 **분석**할 수 있는 **전용 기술**개발

  ※ 피해 시스템 초동대응 특화 기법 및 개인정보 특화 디지털 포렌식 조사 기술 등 연구

❸ 전문인력(CPO 등) 취업 연계 지원

- **(CPO 공급) 관리자 레벨의 CPO** 직무성격, 범위*를 고려하여, 졸업과 동시에 역할 수행이 가능한 인력을 **필요 기관에 직접 매칭**

  * 개인정보 보호 계획 및 처리 실태 관리, 피해구제, 유출 오남용 방지, 교육 등 총괄

- **(취업 연계 지원) 전문인력 수요 기업과의 공동연구** 및 **실무 훈련** 등을 **병행**하여 **취업**부터 실무 **대응역량 강화**까지 **연계**하는 **안정적 지원 환경** 조성

  ※ 지역 연계 및 기업의 수요를 반영한 연구개발·훈련을 통해 즉시 투입가능한 전문가로 양성

❹ 산업계 참여 교과과정 개발

- **(교과목 개발)** 산학협력 등 형태로 **직접 소통**을 통해 **데이터 전처리, AI-PET, 사고 예방·대응 등 산업 현장에서 즉시 필요로 하는 교과목** 개발

- **(다학제적 학문)** 산업에서 **안전한 개인정보 활용**을 위한 관련 기술·법·경영·행정 등 **다분야 학문이 융합된 교과과정**을 운영

- **(사전예방 모의실습) 지역에 특화된 산업**에 맞는 **시나리오 별 개인정보처리시스템**을 **확인·분석**하는 등 **유출 사고 예방 등** 관련 **강의** 개발

개인정보 관련 기술·정책 분야 주요 교과목(예시)

기술	법·제도	관리제도 및 경영관리
· 데이터 프라이버시 기본 개념 및 모델링 · 개인정보 비식별화 기술(가명/익명 처리 기술 등) · 재식별 위험 평가 · 통계기반 PET 모델의 정교화(K-익명성 등) · 차분 프라이버시(DP) 개요 · 암호기반 PET(HE,SMC) · 연합학습(FL) PET 개론 · 합성데이터 PET 개론 · AI-PET 개요 · PET 시스템 엔지니어링(End-to-End) · PET 캡스톤 디자인 · 유노출 최소화 기술 · 개인정보 안전활용 기술 · AI 환경 대응 기술 · 생체정보 등 개인정보 특화 기술 · 새로운 개인정보 원천기술	· 개인정보 보호법 유관 법령(신용정보법, 위치정보법, 인공지능기본법, 데이터산업법 등 개인정보 및 데이터 관련 규율체계) · 해외 법제도(GDPR, CCPA등) · 정보통신망법, 정보통신 기반 보호법 등 정보보호 법제 · 보건·의료, 인사·노무, 클라우드 등 개인정보 관련 규정 · 정보주체의 권리보장을 위한 기본 소양(윤리 등) · 행정조사 제도의 이해 · 개인정보 분쟁조정 개론 · 개인정보 침해요인 분석 방법론 · 정보주체 권리보장(윤리) 개론 · AI 프라이버시의 이해	· 국내 개인정보보호 관리제도(ISMS-P 인증제, 관리수준평가, 개인정보 영향평가, 고유식별정보 실태점검, 개인정보 유·노출 등 상시평가제) · 해외 개인정보보호 관리제도(CBPR, ISO 27701 등) · 기술적·관리적·물리적 안전조치 기준(개인정보의 안전성 확보조치 등) · 개인정보보호 관리체계(기본, 실습) · (위험관리기반)데이터·시스템 전략 경영 · 개인정보 안전·활용 제도 및 체계

학기 별 교육과정(예시)

	1학기	2학기	3학기	4학기
기초	연구방법론	연구지도	개인정보보호세미나	창업 및 진로탐색
기술	현대암호학	개인정보보호 강화기술	프라이버시 기반설계	인공지능과 개인정보보호
	개인정보보호 암호기술의 이해	가명 · 익명처리기술	디지털 포렌식	디지털서비스와 개인정보보호
	개인정보 안전성 확보조치		개인정보보호 유출사고 조사	개인정보 침해사례분석
법제	법학개론	개인정보보호법	개인정보보호분쟁사례	개인정보보호 특별법1(의료)
	인공지능과 법	개인정보보호정책	해외 개인정보보호법	개인정보보호 특별법2(금융)
경영관리	프라이버시와 소비자보호	개인정보보호 관리체계	개인정보영향평가	개인정보보호 거버넌스
			개인정보보호 인증제도	데이터 및 시스템 전략 경영

❺ 이공계·실무경력 교원 확보 및 통계 기반 구축

- **(전임 교원)** 기본적으로 **컴퓨터공학 등 인공지능 관련, 데이터 및 정보보안** 관련 전공 및 **법률, 행정, 경영** 전공 등 교원 확보

- **(산업체 연계) 공공기관, 기업**에서 **개인정보 관련 임원직**을 수행해 본 경험이 있거나 **개인정보 보호·활용 기술 개발 및 상용화 경력**이 있는 교원을 채용하여 **실무감각에 대한 교육**도 가능한 체계 구축

- **(통계조사) 개인정보 산업 규모 대비 전문인력 현황**, 수혜 인력의 졸업 후 경로 등 **성과추적 조사**가 가능한 **각종 통계 설계·연구·조사**

❻ 가명·익명 데이터 등 실습환경 구축

- **(실습 인프라) 개인정보 처리·관리 실습** 및 **PET 상용화 전 단계 모의실험** 등이 가능한 보안 요건을 갖춘 **시설** 등이 구비된 **인프라** 마련

  ※ 개인정보위 지정 '개인정보 이노베이션 존'을 통해 공식적 실습 인프라 활용

- **(실증 연습) 산학연계**로 의료·금융 등 주요 분야별 **개인정보 유노출 공격 대응 실습, 개인정보 포함 데이터 분석, 비식별 처리 연습**

❼ 해외 대학 연계 공동연구 수행

- **(MOU 체결)** 미국, 영국, 캐나다 등 개인정보 보호 법제 및 기술이 발달한 선진국 대학원과 **MOU를 통해 원생 교류 프로그램** 운영

- **(공동연구) 연구실 간 협력**을 통해 새로운 PET, 개인정보 원천기술, 개인정보 보호 표준 등 세부 주제에 대해 **국제공동연구** 진행

❽ AI 신뢰 증진을 위한 기술 표준 선점

- **(표준화 지원) ISO, ITU 등 국제 표준화 기구 표준채택**을 위한 기술 개발, 절차 지원 등 개인정보 표준 선점을 위한 **종합적 지원**

- **(표준 전문가 양성) 개인정보 보호 관련 국제표준 채택**을 위한 산학협력 **표준 개발·채택 절차 경험**을 갖춘 **특화된 전문가 양성**

【 2단계 - 선도기술 연구인재 양성(석·박사급 연구자 등) 】

개인정보 분야 선도기술 연구인재 양성 로드맵(2031~2035, 총 300명 양성)

<table>
<tr><th>양성분야</th><th>지원대상</th><th>2031</th><th>2032</th><th>2033</th><th>2034</th><th>2035</th></tr>
<tr><td rowspan="6">개인정보
선도기술
연구인재 양성</td><td rowspan="3">차세대
개인정보
기술인재
3개교
(180명)</td><td colspan="3">능동형 AI 프라이버시 제어기술 연구</td><td></td><td></td></tr>
<tr><td></td><td colspan="3">신종 AI 융합 서비스 관련 실시간 위험저감 기술 연구</td><td></td></tr>
<tr><td></td><td colspan="3">개인정보 전주기 별 보호방안 연구</td><td></td></tr>
<tr><td rowspan="3">개인정보
융합인재
2개교
(120명)</td><td></td><td></td><td colspan="3">다중 AI 플랫폼의 내재화된 보호기술 연구</td></tr>
<tr><td></td><td colspan="2">개인정보 침해·유출 사전예방 기술 연구</td><td></td><td></td></tr>
<tr><td></td><td></td><td colspan="2">사고 원인·분석 자동화 연구</td><td></td></tr>
<tr><td></td><td></td><td colspan="3">PbD 기반, 프라이버시 융합모델 연구</td></tr>
<tr><td></td><td></td><td></td><td></td><td colspan="2">개인정보 추적·관리 기술 연구</td></tr>
</table>

※ 신규 예산확보 여건에 따라 추진시점과 양성 규모가 일부 변경가능

❾ 차세대 개인정보 강화 핵심기술 분야

- **(AI 특화)** 개인정보 자체를 안전하게 활용하기 위한 기존의 PET 기술을 넘어 AI 환경에 능동적으로 제어가능한 신기술 연구로 확장

- **(위험제어)** 피지컬 AI와 에이전틱 AI가 융합된 신종 서비스 등에서 개인정보의 **대규모 수집 위험 제거** 및 **위험도 경감** 등 기술 연구

※ '①논리 판단→②위험도 검증→③하드웨어 실행' 방식의 검증 절차 기술 등 선행연구

⑩ AI 기반, 개인정보 보호 전주기 보호 기술 분야

- **(전주기 보호)** 시스템 통합(SI) 체계와 결합된 신종 AI 플랫폼 등의 **개인정보 전주기 별 흐름 통제 및 다중 AI 환경의 보호 방안** 등 연구

  ※ (예시) 플랫폼 내 AI 에이전트 간 과도한 개인정보 수집·가공·학습·공유·파기 등을 사전인지 및 재식별 위험을 제거하는 등의 선행연구 수행 필요

- **(아키텍처)** 의료, 공공 등 산업분야 별 **특화된 버티컬 AI 기술**의 개인정보 처리 오작동 등 방지를 **내재화된 아키텍처** 등 **연구·설계**

  ※ 산업분야 별 특화된 개인정보 최소수집 및 특화된 재식별 위험제거 방법론 등 정립

⑪ 개인정보 특화 유출사고 예방·조사 선도기술 분야

- **(사전예방)** 개인정보처리시스템의 내·외부 위협 및 안전성 확보 여부를 **상시 점검**하고 **예방**할 수 있는 **자동화 기술** 등 **연구개발**

- **(원인규명)** 개인정보 유출 관련, 사고원인 규명 및 현장분석 기술, 대용량 융합데이터 분석 등 **행정조사 특화 기술연구 등 고도화**

  ※ 각종 보안시스템 로그 분석, 특정 사용자 별 행위 추적 등이 융합된 심층분석 기술 등

⑫ 신산업 융합 개인정보 보호·활용 기술 분야

- **(추적·관리)** 피지컬 AI·로봇 등 신기술이 적용되는 산업의 개인정보 처리 관련 **책임 추적성**(Accountability) **강화**를 위한 **선도기술 연구개발**

  ※ 감사로그(Logging) 및 데이터 흐름 추적(Data Lineage) 등 자동화 방안 연구 등

- **(융합모델)** 개인정보보호 중심 설계(PbD) 기반으로 **신산업**에 적용 가능한 **개인정보 보호** 및 **안전활용 융합 모델 연구개발**

  ※ 온디바이스(On-Device) 환경의 개인정보 비식별화 및 실시간 안전성 검증 방법론 연구 등

산업의 수요에 대응 가능한 **개인정보 보호·활용 전문인력**을 **양성**하여 **민·관·연 선순환 생태계**를 **조성**하고, 개인정보 특화 **연구자 양성**으로 대상을 확대함으로써 **신산업에 부합하는 인재**를 **지속 발굴**

Ⅴ 기대효과

개인정보에 특화된 기술개발 및 글로벌 수준의 전문인력 양성으로 **국내·외 개인정보 산업 육성, 개인정보 법·기술 정책 고도화**

- 산업현장 맞춤 개인정보 특화 기술개발로 **개인정보 관련 산업**의 **전방위적 확대·성장**을 통한 경제적 효과 창출

AI 등 신기술 관련 **공공·민간 애로사항 해결** 및 **현장 인력난 해소**

- 신기술 도입 시 **도메인별 개인정보 이슈 파악·해결이 상시 가능한 체계**를 구축하여, **혼란 없는 AI·데이터 시대로 진입**

국제 수준의 연구 기회를 제공하여 **학문적 위상 제고**

- 개인정보 분야에 특화된 창의적인 연구가 가능하여 세계적인 경쟁력을 확보하고, 영속성 있고 전문화된 학문분야로 정착

개인정보 분야 **학제 간 융합 가능한 연구환경**으로 안착

- ICT·법·정책·사회과학·윤리 등 학제 간 단순 병렬이 아닌 상시 보호·활용, 사고예방·사후대응 등 **전주기 별 융합 가능한 연구체계** 구축

개인정보 보호·활용 전문가 확산을 통한 **체계 선도국**으로 **도약**

- 사회 전반에 걸친 개인정보 보호수준 향상 및 안전한 활용 기반을 마련하여 **프라이버시 분야 선도국가로 발돋움**

붙임 용어 정의

- **개인정보보호 강화 기술(PET, Privacy Enhancing Technologies)** : 개인정보가 재식별되지 않도록 조치하면서 안전하게 데이터를 활용할 수 있도록 지원하는 개인정보 보호 및 정보통신(ICT) 기술
- **개인정보 지갑(Personal Data Wallet)** : 나의 신원·자격·개인정보를 한 곳에 안전하게 보관하고, 필요한 서비스에만 선택적으로 내 정보를 외부로 발송하거나 철회할 수 있도록 지원하는 전자 지갑
- **자기주권신원(SSI, Self-Sovereign Identity)** : 신원정보를 국가나 기업이 아니라 본인이 직접 보관·관리하고, 필요할 때만 일부를 증명할 수 있게 지원하는 디지털 신원 방식
- **탈중앙식별자(DID, Decentralized Identifier)** : 중앙 기관에 등록하지 않고도 블록체인 등 분산 시스템을 통해 스스로 발급·검증할 수 있는 새로운 형태의 신원 식별자
- **딥페이크(Deep fake)** : 인공지능을 이용해 실제 인물의 얼굴·목소리 등을 정교하게 합성해 만든 가짜 이미지·영상·음성
- **삭제 증명(Proof of Erasure)** : 어떤 데이터를 완전히 지웠다는 사실을 기술적으로 입증하고, 나중에 다시 확인할 수 있게 해 주는 증명 기술
- **양자내성 암호화(Post-Quantum Cryptography)** : 양자컴퓨터를 이용하여 연산을 진행하여 쉽게 해독되지 않도록 설계된 차세대 암호 기술
- **신뢰실행환경(TEE, Trusted Execution Environment)** : 컴퓨터·스마트폰 안에 일반 영역과 분리된 '보안 전용 구역'을 만들어, 중요한 코드와 데이터를 안전하게 처리하는 하드웨어 기반 기술
- **엣지 디바이스(Edge Device)** : 클라우드 서버가 아닌 사용자 가까운 곳(단말·IoT 기기 등)에서 데이터를 직접 수집·처리하는 장치
- **제로트러스트(Zero Trust)** : 내부·외부를 막론하고 누구도 기본적으로 신뢰하지 않고, 매번 접속 주체를 확인·검증한 후에만 접근을 허용하는 보안 개념
- **다크웹·표면웹(Dark Web, Surface Web)** : 일반 검색엔진으로 보이는 일반 웹을 표면웹, 특정 브라우저 등 별도 프로그램으로만 접속 가능한 음성화된 거래·사이트 영역을 다크웹으로 정의
- **공개출처정보(OSINT, Open-Source Intelligence)** : 인터넷·뉴스·SNS·공공데이터 등 누구나 볼 수 있는 공개 정보를 모아 분석해 획득하는 정보
- **퍼셉추얼 해시(Perceptual Hash)** : 이미지·문서의 내용을 기준으로 비슷한 파일끼리 비슷한 값이 나오도록 만든 특수한 해시값으로, 동일하거나 매우 유사한 콘텐츠를 찾아내기 위한 기술
- **합성데이터(Synthetic Data)** : 실제 사람의 정보를 직접 쓰지 않고, 통계적 특성만 비슷하게 인공지능 등으로 만들어 낸 익명화 처리된 데이터
- **동형암호(HE, Homomorphic Encryption)** : 데이터가 암호화된 상태에서 연산을 수행하고, 결과만 복호화하여 활용하는 방식의 암호 기술

- **안전한 다자간 연산(MPC, Multi-Party Computation)** : 각 기관 별로 보유한 데이터는 공유하지 않고, 합계·모델 결과 등 필요한 계산 결과만 함께 전달하는 연산 기술
- **기밀 컴퓨팅(Confidential Computing)** : 클라우드나 서버 안에서도 운영자조차 데이터를 열람할 수 없도록, 하드웨어로 연산 과정까지 암호화 및 격리하는 기술
- **차분 프라이버시(DP, Differential Privacy)** : 통계·AI 결과에 작은 '노이즈'를 추가하여 특정인을 식별하거나 알아볼 수 없게 만드는 수학적 프라이버시 보호 기법
- **데이터 클린룸·데이터스페이스(Data Clean Room Dataspace)** : 원본 데이터는 각 기관에 둔 채, 외부로 반출하지 않고 정해진 규칙 안에서만 결합·분석할 수 있도록 지원하는 안전한 데이터 활용 공간·연결 구조
- **언러닝(Unlearning)** : 이미 학습된 인공지능 모델에서 특정 데이터의 영향만 골라 제거하는 등 첫 단계부터 해당 데이터를 학습하지 않은 것과 유사하게 만드는 기술
- **연합학습(FL, Federated Learning)** : 데이터를 한 곳에 모으지 않고 여러 단말·기관이 각자 학습한 결과(모델 파라미터)만 모아 공동 모델을 만드는 분산된 환경의 학습 방식
- **정렬 파인튜닝(Alignment Fine-Tuning)** : 인공지능이 법·윤리·사회 규범과 사람 선호에 더 맞는 답을 하도록, 사람 피드백 등을 이용해 모델을 다시 조정하는 학습 과정
- **설명가능·감사가능 AI(XAI·Auditable AI)** : 인공지능이 어떤 이유로 그런 판단·출력을 했는지를 사람이 이해·설명하고, 외부에서 점검·감사할 수 있도록 설계된 AI
- **가드레일(Guardrail)** : 인공지능이 위험한 요청을 받거나 위험한 답을 하려 할 때, 이를 필터링·수정·차단해 안전한 범위 안으로 유도하는 보호 장치
- **콘텐츠 출처 및 진위 보장을 위한 국제 협의체(C2PA, Coalition for Content Provenance and Authenticity)** : 디지털 이미지·영상·문서의 생성·수정 이력을 기록·검증하기 위한 산업 주도 공개 기술규격 및 표준사양을 개발하는 협의체
- **프로비넌스(Provenance)** : 특정 디지털 콘텐츠가 누구에 의해, 어떠한 과정을 거쳐 생성·편집·전달 되었는지에 대한 '출처 이력' 정보
- **AI 개인정보 비서(AI Personal Data Assistant)** : 사용자의 동의·열람·삭제 요청을 대신 처리하고, 여러 서비스에 흩어진 개인정보 이용 현황과 위험을 알려주는 AI 기반 비서
- **모델 컨텍스트 프로토콜(MCP, Model Context Protocol)** : AI 모델이 외부 데이터베이스, 도구·서비스와 표준화된 방식으로 연결되어 정보를 송·수신하는 규약
- **피지컬 AI(Physical AI)** : 로봇·드론·센서 장비처럼 물리적인 상태 및 환경에서 움직이거나 감지·조작을 수행하는 AI 시스템
- **비전-언어모델(VLM, Vision-Language Model)** : 이미지·영상 같은 시각 정보와 텍스트를 함께 이해하고, 두 가지를 연결해 설명·질의응답 등을 수행할 수 있는 인공지능 모델
- **공급망(Supply Chain, 개인정보 관점)** : '개인정보 제공자–처리기관–클라우드·플랫폼–솔루션·협력사–외부위탁사–제3자 제공' 등으로 이어지는 개인정보 처리 전 과정을 말하며, 한 지점의 취약점·침해가 연쇄적으로 확산될 위험성 존재

2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵

발 행 일 2026년 6월
발 행 처 개인정보보호위원회
지 원 기 관 한국인터넷진흥원
디 자 인 봄날커뮤니케이션

※ 최신자료는 '개인정보보호위원회 누리집(pipc.go.kr)', '개인정보 포털(privacy.go.kr)'에서 확인할 수 있습니다.

2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵

개인정보보호위원회
Personal Information Protection Commission