2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵 요약본

개인정보보호위원회
Personal Information Protection Commission

2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵 요약본

개인정보보호위원회
Personal Information Protection Commission

2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵 요약본

목 차

1 추진배경

인공지능(AI)·데이터 경제가 성장하면서 규율환경이 변화

- 국내 데이터 산업의 성장으로 개인정보 보호에 필요한 법·정책*, 각종 안내서 등 안전한 활용을 가능하게 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 약 50억 달러('26년, 한화로 약 7.5조원)에서 312억 달러('34년, 약 47조원)까지 성장할 것으로 예측

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

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

  ※ (국내) 개인정보 보호 관련, 최우선 정부정책으로 기술개발·보급을 공공·민간 부문 모두 상위권 차지
  (국외(OECD, 英 ICO 등)) PET가 개인정보 보호 규제 준수와 신뢰 기반의 AI 모델 공유에 필요한 핵심 요소

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

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

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

  ※ 특히, AI는 새로운 분야로 정립하고, 향후 발전을 고려한 기술 R&D와 표준화 방향을 설정하여 개인정보의 침해·유출 위험을 낮출 필요

기술개발 성과가 글로벌 표준으로 이어질 수 있도록 종전의 기술 R&D, 표준화 로드맵을 하나로 통합·연계하여 체계적인 확산 추진

2 R&D 관련 정책·기술 및 시장 동향

【 국내 환경 】

(정책) 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

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

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

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

(기술·표준) 공공·금융·의료분야의 실증환경에 PET가 활용 중이고, 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

- 정부의 지원을 통해 '연구·국제표준화→실증→민간'으로 이어지는 선순환 구조 조성을 위하여 PET의 단계적 확산 전략을 추진 중

- '가명·익명처리, 동형암호, 분산형 ID 등' 프라이버시 기술의 표준화가 확대 중이며, ISO/IEC 국제표준 중 일부를 채택·적용*

  * 대표적인 국내 표준화 추진 기관: 한국정보통신기술협회(TTA), 한국산업표준(KS)

【 국외 환경 】

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

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

  ※ NSTC에서는 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

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

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

  ※ (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

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

(기술·표준) PET는 개인정보를 공개하지 않은 상태에서 연산·분석을 수행할 수 있는 기술로써 실 서비스에 탑재하여 상용화하는 추세

- **(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

- **(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

- **(표준규격)** 국제 표준기구에서는 PET 관련 용어·참조 아키텍처·기술 규격을 표준화하여 글로벌 상호운용성과 인증 체계 마련 중

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

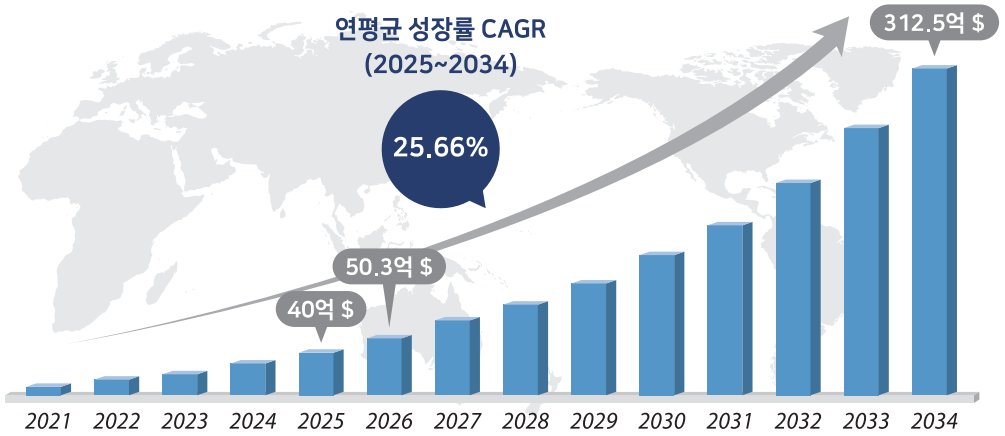
【 시장·산업 동향 】

● **(전 세계 PET 시장)** 글로벌 리서치 기업의 PET 시장 규모 및 전망에 따르면 전 세계 시장 규모는 '34년까지 약 312억 달러(매년 약 25.6% 성장) 예상

※ ('26년) 50억 3천만 달러 → ('34년) 312억 5천만 달러(한화로 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

※ (산식) 국내 정보보안('23) 6.145조 원 × 글로벌 PET 비중(1.9-2.5%) × PET 연평균 성장률(25.66%)

● 산업 동향

- **(국내)** 다양한 PET 솔루션이 의료·금융 중심으로 빠르게 확산 중

※ 일부 기업은 글로벌 수준의 개인정보 보호·활용 기술을 적용하여 서비스로 운영 중

- **(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

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

* 개인정보 분야의 산·학·연 전문가(22인)를 대상으로 기술 수요조사 및 분류체계 설문 등 병행

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 현장에서 개인정보보호를 작동시키는 데 필요한 핵심기술과 구성·운영 요소*을 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

- 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

• 중분류(4)-소분류(15)-세분류(59)로 구분 및 개인정보 생애주기와 연계 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	●	●	●	●	

4 R&D 추진전략

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

개인정보 보호·활용 AI 서비스 시장 확대	시장 확산	인재 양성	AI·PET 전문 인재 양성 및 일자리 창출
AI·PET 융합 R&D 기술·표준 개발	기반 구축	정책 연계	국제 표준 연계 및 법·제도 고도화

AI-친화적 개인정보 보호·활용 생태계 조성

5 최종 선정된 로드맵 대상 핵심기술 및 표준

「개인정보 R&D 중장기 로드맵 개정 연구」를 통해 수요조사를 실시하였고, 전문가 자문반을 구성하여 핵심기술 11개 최종 선정

- 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

- 또한, 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

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

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

6 기술개발 및 표준화 로드맵

(범례) : 세부 기술 : 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="3">1 개인정보 주권 보장</td><td rowspan="3">1-2 정보주체 통제권</td><td rowspan="3">① 정책 준수 증명 결과 열람</td><td></td><td colspan="3">개인정보 활용 현황을 모니터링하고 통제권 실행 을 보장하는 기술</td><td></td></tr>
<tr><td></td><td colspan="3">검색증강생성(RAG) 프라이버시 기반 개인정보 보존형 검색(Retrieval) 및 실시간 삭제 증명(Forget-by-Design) 기술</td><td></td></tr>
<tr><td colspan="5">[국제표준] 소비자 권리 보호를 위한 PbD 관련 국제표준</td></tr>
<tr><td rowspan="6">2 유·노출 위험 경감</td><td rowspan="3">2-1 수집 시 개인정보 탐지</td><td rowspan="3">② 딥페이크/합성 검증·레이블링</td><td colspan="2">딥페이크 사전 예방을 위한 데이터 변환 기술</td><td colspan="2"></td></tr>
<tr><td></td><td colspan="2">저위험 비식별 음성데이터 기반 보이스피싱·딥페이크 지능형 탐지·차단 및 안전활용 통합 기술</td><td></td></tr>
<tr><td></td><td colspan="4">[국제표준] 딥페이크·합성콘텐츠 진위검사 결과를 기록·공유하기 위한 공통 메타데이터 항목 및 화면 표시 방식 국제표준</td></tr>
<tr><td rowspan="3">2-3 개인정보 안전성 확보</td><td rowspan="3">④ 엣지 디바이스 개인정보보호</td><td></td><td colspan="2">온디바이스 격리 환경에서의 개인정보 이상행위 탐지 및 자동 통제 기술</td><td></td></tr>
<tr><td colspan="2"></td><td colspan="3">[국제표준] 엣지·모바일 단말 환경에서 개인정보보호를 위한 보안 아키텍처·접근통제 요구사항 국제표준</td></tr>
<tr><td colspan="2"></td><td colspan="3">[국내표준] 온디바이스 개인정보 이상행위 탐지·차단 기능 및 로그 관리에 관한 시험·평가기준 국내 표준</td></tr>
</table>

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		
					[국제표준] 가명·비식별 정보 재식별 위험도 평가 방법론 및 지표에 관한 국제표준		
					[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·참조 모델 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="4">4-4 AI 에이전트 보안</td><td rowspan="4">③ 피지컬 AI 실시간 프라이버시 제어</td><td colspan="2"></td><td colspan="2">피지컬 AI·로봇 융합 환경을 위한 프라이버시 인지형 신원·행동 관리 및 최소수집 기술</td><td></td></tr>
<tr><td colspan="3"></td><td colspan="3">로봇·IoT 등 실환경에서 개인정보 안전교환 프로토콜 및 상호작용 기술</td></tr>
<tr><td colspan="3"></td><td colspan="3">[국제표준] 로봇·IoT·스마트기기의 센싱·저장·전송 단계별 프라이버시 보호 설계·운영 가이드라인 국제표준</td></tr>
<tr><td colspan="3"></td><td colspan="3">[국내표준] 피지컬 AI 서비스에 대한 프라이버시 영향평가(PIA)·위험등급 분류 및 인증 기준 국내표준</td></tr>
<tr><td rowspan="4">4-5 AI 기반 개인정보 탐지·비식별화</td><td rowspan="4">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="3"></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="3"></td><td colspan="3">[국제표준] AI 기반 비정형데이터 개인정보 탐지·비식별화 성능 평가용 벤치마크·지표·시험방법 국제표준</td></tr>
<tr><td colspan="3"></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

붙임 개인정보 보호·활용 기술 개념 및 정보보안 기술과의 관계

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

※ 예시: 정보주체의 권리보호 기술은 정보보안 기술의 영역에 미포함되는 신분야

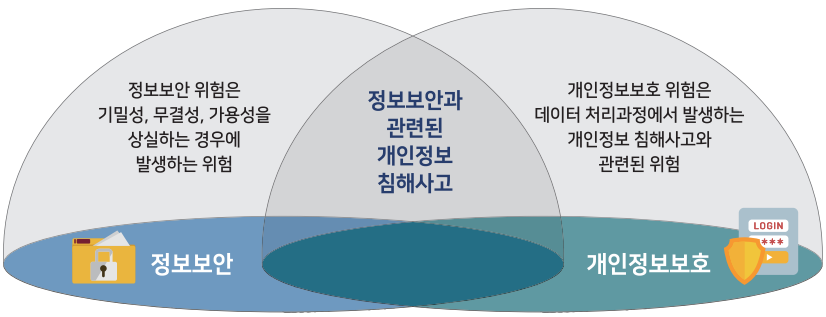
개인정보 보호·활용 기술과 정보보안 기술 비교

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




Personal
Information
Protection
Privacy

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 가능성

※ 개인정보를 보호하면서 AI 개발에 활용하는 능력이 핵심 성공 요인으로 부각

복잡·다양하게 진화하는 AI의 특성에 맞추어 개인정보 활용의 「안전밸브」역할을 수행할 고급 인력 양성이 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 심각성은 더욱 커질 가능성이 증가하여 고급 인력 수요가 급증 예상

전 세계는 안전하게 개인정보를 AI에 활용하는 것이 글로벌 AI 경쟁력의 원천임을 인식하고 개인정보 인력 양성에 집중 투자

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

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

AI 기술 발전으로 인해 예측 불가능한 형태로 유출 보안 위협이 진화하고, 개인정보 처리 자동화·집중화로 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 시대에 맞는 성숙한 개인정보 리스크 관리 체계를 갖추지 못하고 있어, 국내 대규모 사고 재발 우려 심각

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

Ⅱ 국내·외 추진현황

국내 교육기관(대학)의 인력양성 및 연구지원 사업 현황

- 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 학부과정* 운영('25.2. 종료)

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

- ITRC(대학ICT연구센터)과 BK21(4단계 두뇌한국21)과을 통해 ICT 및 정보보안 분야 연구역량 제고를 위한 연구지원 사업이 진행 중

  - **(ITRC)** AI, 6G, 반도체, 양자통신 등 미래 ICT 핵심기술 연구 지원, 석·박사급 ICT 고급 연구인력 양성 및 산학협력 활성화

  - **(BK21)** 세계적 수준의 연구중심대학 육성, 대학원 연구역량 제고 및 안정적인 연구비 지원

국외 교육기관(대학)의 인력양성

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

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

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

- '미국, EU, 싱가포르, 일본'에서는 정부차원에서 석·박사급 우수 인재 양성을 위하여 연구비 등을 지원하는 프로그램을 운영 중

  ※ 미국 국립과학재단, EU Horizon Europe, 싱가포르 과학기술연구청, 일본학술진흥회(JSPS)

Ⅲ 시사점 및 전문인력 양성 방향

전 세계적으로 AI 신뢰성, 데이터 안보에 대한 정부 지원 가속화, 동시에 프라이버시가 주요 이슈로 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)

- 과징금 처분 본격화*에 맞춰 개인정보 전문인력 확보를 통한 법 위반행위 예방·대응 체계로 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 지원하여 공공·민간의 대응력 향상 필요

- 개인정보 보호책임자(CPO) 역할 강화, 자격요건 법정화('24.3.)*로 급증한 전문인력 수요를 교육 시장의 자발적인 전공 개설 및 인력 배출만으로 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

지속 제기된 민간·공공기관 개인정보 전문인력 수요에 부응할 필요

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

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="10">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="5">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

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="7">개인정보
선도기술
연구인재 양성</td><td rowspan="4">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></td><td></td><td colspan="3">다중 AI 플랫폼의 내재화된 보호기술 연구</td></tr>
<tr><td rowspan="3">개인정보
융합인재
2개교
(120명)</td><td></td><td colspan="3">개인정보 침해·유출 사전예방 기술 연구</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

- **(추척·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**

2026 ~ 2030

개인정보 전주기 보호·활용 기술 R&D 및 표준화 로드맵 요약본

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

※ 최신 로드맵 전체본은 '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 요약본

개인정보보호위원회
Personal Information Protection Commission