KISA 한국인터넷진흥원

PRIVACY REPORT

2025년도 개인정보 기술동향

PRIVACY REPORT 2025년도 개인정보 기술동향

1. 인공지능(AI) 기술 · 3

2. 개인정보 보호 강화 기술(PETs) · · · · · · · · · · · · · · · 12

3. 생체인식 기술·디지털 신원 · · · · · · · · · · · · · · · · · 20

4. 연령 확인 및 아동보호 · · · · · · · · · · · · · · · · · · · 27

5. 데이터 활용 기술 · 33

1. 인공지능(AI) 기술

(1) 개인정보위, AI 개발에 원본 데이터 활용 특례 신설 및 딥페이크 규제 강화

(2) EU: EDPB, 인공지능 편향성과 정보주체 권리 보장에 관한 보고서 발표

(3) EU: AI법에 따른 AI 시스템 정의에 관한 가이드라인 발표

(4) OECD, AI 사고 대응을 위한 글로벌 보고 프레임워크 마련

(5) EU: EDPB, LLM의 프라이버시 리스크 관리 프레임워크 보고서 발간

(6) ISO, AI 영향평가 기준 표준 발표

(7) 프랑스: CNIL, AI 학습용 데이터 처리의 적법성 기준 권고안 발표

(8) EU: EDPS, 인공지능 시스템 위험관리 지침 발표

1월 개인정보위,
AI 개발에 원본 데이터 활용 특례 신설 및 딥페이크 규제 강화

❖ 주요 내용

- 2025년 1월 13일, 개인정보위는 '2025년 주요 정책 추진계획'을 통해 자율주행 AI 등에서 가명정보만으로 연구 목적 달성이 곤란한 현실을 인정하고, 적정한 안전조치 + 개인정보위 심의·의결을 전제로 원본 정보 활용을 허용하는 개인정보 보호법 특례 규정 마련을 추진함. 이는 고도화된 AI 개발을 위한 필수 요건인 고품질 원본 데이터의 제한적 활용을 제도적으로 보장하는 정책
- 또한 AI 개발 사업자가 '정당한 이익' 또는 공익을 기반으로 개인정보를 처리할 수 있도록 적법 처리 근거 확대를 병행하여, 산업 현장에서 요구되는 합리적 정보 활용 범위를 구체화하고자 함.
- 딥페이크(Deepfake) 악용 사례 확산에 대응하기 위해 정보주체의 삭제 요구권 도입, 인격적 가치를 훼손하는 합성 정보 금지 및 처벌 규정 마련을 추진함으로써 인격권 보호 중심의 규범 체계를 강화
- 영상정보 활용 증가에 따라 「영상정보처리기기 설치·운영 등에 관한 법률(가칭)」 제정을 통해 영상정보 처리 기준, 안전장치, 권리 보호 체계를 별도 법률로 정비하려는 움직임도 포함됨.
- 아울러 가명처리 적정성 심의위원회를 법제화하고, 비정형 데이터(영상·음성·이미지 등)의 가명처리 기능을 강화하며, 개인정보 보호 강화기술(Privacy Enhancing Technologies, PETs) 연구개발 지원을 확대하는 등 AI 생태계 전반의 정보 활용 기반 확충 방안도 제시됨.

출처:
· 개인정보위, "AI 개발에 원본 데이터 활용 특례 신설…딥페이크 규제 강화" (전자신문, 2025.01.13.)
https://n.news.naver.com/mnews/article/030/0003275607?sid=105
· 안전한 개인정보, 신뢰받는 인공지능 시대 -「2025년 개인정보보호위원회 주요 정책 추진계획」 발표 (개인정보위, 2025.01.13.)
https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=10928

1월 EU: EDPB, 인공지능 편향성과 정보주체 권리 보장에 관한 보고서 발표

❖ 주요 내용

- 2025년 1월 23일, EU 개인정보보호이사회(European Data Protection Board, EDPB)는 인공지능 편향성과 정보주체 권리 보장을 다룬 「효과적인 정보주체 권리 보장(Effective Implementation of Data Subjects' Rights)」과 「편향 평가(Bias Evaluation)」 보고서를 발간
- 해당 보고서는 독일 연방 개인정보 감독기관(Federal Commissioner for Data Protection and Freedom of Information, BfDI)의 요청에 따라 전문가 지원 프로그램(Support Pool of Experts)을 기반으로 작성됨.
- 보고서는 AI 시스템의 편향 발생 구조와 정보주체 권리 보장의 기술적 제약을 종합적으로 분석함. 특히 AI 감독 체계를 구성하는 핵심 요소로서 편향 완화, 데이터 삭제 및 학습취소(Unlearning)* 구현 가능성, 생성형 AI의 개인정보 출력 제한 등을 주요 과제로 제시

  * 학습 취소(Unlearning): 모델이 특정 데이터의 학습 효과를 제거하거나 영향력을 감소시키도록 수정하는 과정.
- 편향 평가(Bias Evaluation) 보고서는 데이터 편향(역사적·대표성), 알고리즘 편향, 평가 편향, 얼굴 인식 기술 편향, 생성형 AI 편향 등 다양한 유형을 제시함. 단순히 민감 변수를 데이터 세트에서 제거하는 방식은 편향 완화에 효과적이지 않다고 명시
- 편향 완화 방식은 사전 처리(pre-processing), 처리 중(in-processing), 사후 처리(post-processing)로 구분되며, 생성형 AI 대응을 위해 데이터 명세서(Data Statements), 사전학습모델 미세조정(Fine-Tuning), 학습데이터 수정, 강화학습 기반 인간 피드백(Reinforcement Learning with Human Feedback, RLHF) 등이 제안됨. 다양한 편향 탐지 도구가 소개되었으나, 생성형 AI 편향을 완전히 해결할 수 있는 기술은 아직 존재하지 않는 것으로 평가됨.
- 효과적인 정보주체 권리 보장 보고서는 데이터가 모델에 미치는 영향을 추적하기 어렵고, AI 학습이 확률적·점진적으로 이뤄진다는 특성 때문에 삭제·학습취소가 구조적으로 어려운 문제를 지적함. 데이터 관리(Data Curation), 출처 추적(Provenance), 전체 모델 재학습(Retraining) 등이 가능한 방안으로 제시되나, 전체 재학습은 비효율적이라는 점도 함께 언급됨.
- 이에 대한 대안으로 모델 비종속 학습취소(Model-Agnostic Unlearning), 모델 내재적 학습취소(Model-Intrinsic Unlearning), 애플리케이션 기반 학습취소(Application-Specific Unlearning) 등 보다 정밀한 접근법이 제시됨. 또한 근사적 학습취소(Approximate Unlearning)**, 차등 프라이버시(Differential Privacy)***, 모델 폐기(Model Retiring) 등 개별 데이터 영향력을 최소화하는 방식도 검토됨.

  ** 근사적 학습취소(Approximate Unlearning): 데이터를 실제 삭제하지 않고 그 영향만 통계적으로 약화시키는 방식.

  *** 차등 프라이버시(Differential Privacy): 노이즈 주입 등을 통해 개별 데이터의 기여도를 식별할 수 없도록 보호하는 기법.
- 생성형 AI의 개인정보 출력 제한과 관련해서는 확산모델(Diffusion Models) 미세 조정, GAN 기반 데이터 수정, 특정 이미지 생성을 차단하는 출력 조정(Output Modification) 등이 권장됨. 보고서는 이러한 기술적 조치가 정보주체 권리 보호와 AI 책임성 강화에 기여할 수 있음을 강조

출처:
- EU: EDPB publishes reports on AI and effective data protection supervision (DataGuidance, 2025.01.24.) https://www.DataGuidance.com/news/eu-edpb-publishes-reports-ai-and-effective-data
- AI-Complex Algorithms and effective Data Protection Supervision (EDPB, 2025.01.23.) https://www.edpb.europa.eu/system/files/2025-01/d1-ai-bias-evaluation_en.pdf

2월 EU: AI법에 따른 AI 시스템 정의에 관한 가이드라인 발표

❖ 주요 내용

- 2025년 2월 6일, EU 집행위원회(European Commission, EC)는 「EU AI법(AI Act)」 제3조(1)에 규정된 'AI 시스템(AI System)'* 개념을 명확히 하기 위한 「가이드라인(Commission Guidelines on the definition of an artificial intelligence system established by Regulation (EU) 2024/1689 (AI Act))」을 발표함. 본 가이드라인은 AI 시스템 정의가 적용 범위, 규제 대상 여부를 판단하는 핵심 요소라는 점을 고려해 마련되었으며, AI 시스템의 구조적 특성과 수명주기 구분을 종합적으로 설명

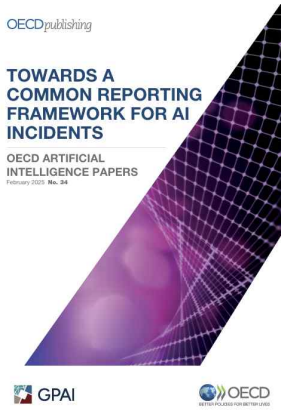
  * AI 시스템(AI System): AI법 제3조(1)에 따라 입력을 기반으로 추론하여 예측·콘텐츠·추천·결정을 생성하고, 물리적·가상 환경에 영향을 미치는 기계 기반 시스템.

- 가이드라인은 AI 시스템을 기계 기반(machine-based) 구조 위에서 작동하는 시스템으로 규정하며, 단순 소프트웨어 대비 AI 시스템의 기술적 차이를 분명히 제시함. 기계 기반은 하드웨어와 소프트웨어가 모두 포함되며, AI 시스템이 계산 중심(computationally driven) 구조임을 강조
- 두 번째 요소인 자율성(autonomy)은 시스템이 일정 수준의 인간 개입 없이 동작할 수 있는 능력을 의미함. 가이드라인은 완전 자율성을 요구하지 않으며, "일정 수준의 독립성(some degree of independence)"만으로도 AI 시스템 범주에 포함될 수 있음을 명시함. 또한 단순 규칙 기반 시스템은 해당되지 않으며, 시스템이 외부 환경에 반응하여 결과를 산출하는 구조를 갖추는 것이 핵심 요건
- 세 번째 요소인 적응성(adaptiveness)은 배포 이후 시스템의 동작이 스스로 변화할 수 있는 성질을 의미하나, 적응성을 반드시 갖춘 경우에만 AI 시스템으로 인정되는 것은 아님. 즉, AI 시스템은 적응성을 가질 수도 있고 가지지 않을 수도 있으며, 이는 정의의 필수 요소가 아니라 선택적 요소로 규정됨.
- 가이드라인은 또한 AI 시스템이 명시적 또는 암묵적 목표(objectives)를 기반으로 작동하며, 입력을 바탕으로 추론(inference)을 수행하여 결과를 생성해야 한다고 명시함. 추론은 AI 시스템을 기존 소프트웨어와 구별하는 핵심 요소로, 머신러닝·딥러닝·강화학습·지식 기반 시스템 등 다양한 AI 기법을 포함한다는 점을 강조
- 보고서는 시스템의 산출(output)이 예측(predictions)·콘텐츠(content)·추천(recommendations)·결정(decisions) 네 범주 중 하나 이상에 해당해야 하며, 이 출력이 물리적 또는 가상 환경에 영향을 미쳐야 함을 정의의 구성 요소로 제시함. 생성형 AI가 생성하는 텍스트·이미지·음악과 같은 콘텐츠 역시 AI 시스템 출력 범주에 해당
- 마지막으로 AI 시스템은 배포 환경과 상호작용하며 환경에 실질적 영향을 미치는 특성을 가져야 한다고 규정함. 상호작용은 로봇·IoT 등 물리적 공간뿐 아니라 소프트웨어·플랫폼·데이터 흐름 등 디지털 환경 모두를 포함함. 이러한 기준은 단순 자동화 시스템이나 통계 처리 시스템 등 '기본 데이터 처리(basic data processing)' 수준의 시스템은 AI 시스템으로 보지 않는 경계를 제시

출처:
- EU: Commission publishes Guidelines on AI system definition under AI Act (DataGuidance, 2025.02.07.) https://www.DataGuidance.com/news/eu-commission-publishes-guidelines-ai-system
- The Commission publishes guidelines on AI system definition to facilitate the first AI Act's rules application (EC, 2025.02.06.) https://ec.europa.eu/newsroom/dae/redirection/document/112455

2월 OECD, AI 사고 대응을 위한 글로벌 보고 프레임워크 마련

❖ 주요 내용



- 2025년 2월 28일, 경제협력개발기구(Organisation for Economic Co-operation and Development, OECD)는 전 세계적으로 증가하는 알고리즘 차별, 개인정보 침해, 보안 취약점 등 AI 관련 사고에 대응하기 위해 'AI 사고 보고를 위한 공통 프레임워크(Towards a common reporting framework for AI incidents)' 보고서를 발표함. OECD는 AI 기술 확산에 따라 사고가 복잡하고 국제적으로 확산되는 특성이 강해지고 있어, 국가별 보고 체계의 단절을 해소하고 글로벌 기준을 마련할 필요성을 강조
- 보고서는 'AI 사고(AI incident)'*와 'AI 위험(AI hazard)'** 개념을 명확히 정립하며, 사고 보고 체계 구축의 기초로 삼을 것을 제안함. OECD는 AI 사고를 개발·운영·오작동 과정에서 발생하여 개인·집단의 신체적 피해, 기본권 침해, 중요 인프라 장애, 개인정보 침해 등을 직접적으로 초래하는 사건으로 정의함. 반면 AI 위험은 사고로 이어질 개연성이 있는 사건·상황으로, 보안 취약점이나 예측 불가한 시스템 동작이 포함됨.

  * AI 사고(AI Incident): AI 시스템의 개발·운영·오작동 과정에서 발생해 개인·집단의 신체적·사회적·경제적 피해 또는 기본권 침해를 직접 유발하는 사건.

  ** AI 위험(AI Hazard): AI 사고로 이어질 가능성이 있는 사건·상황으로, 보안 취약점·예측 불가한 시스템 동작 등 포함.
- 특히 실시간 데이터 학습·업데이트 기능을 가진 AI 시스템은 예측하지 못한 방식으로 동작할 가능성이 있어 지속적 모니터링이 필요하다고 지적함. 이러한 위험 요소는 단일 제품의 오류를 넘어, 연쇄적 사고나 복합 사고를 유발할 수 있어 국제적 공조가 필수적
- 사고 보고 프레임워크 설계를 위해 OECD는 ▲OECD AI 시스템 분류 프레임워크 ▲AI Incidents Database (AIID)*** ▲OECD 글로벌 제품 리콜 포털 ▲AIM(AI Incidents Monitor)****를 핵심 자료를 활용함. 이 자료들은 사고 유형 분석, 국가 간 비교, 초기 대응 체계 구축 등 국제적 협력을 위한 기반으로 설명됨.

  *** AI Incidents Database(AIID): 전 세계 AI 사고 사례를 수집해 분석·공유하는 공개 데이터베이스.

  **** AI Incidents Monitor(AIM): AI 사고 발생을 추적하고 사고 지표를 모니터링하는 OECD 기반 시스템.
- 보고서는 사고 보고 프레임워크를 구성하는 총 29개 기준(criteria)을 제시하고, 이 중 7개를 필수 요소(mandatory)로 지정함. 필수 요소에는 ▲사고 제목 ▲사고 설명 ▲관련 시스템 정보 ▲보고자 정보 ▲사고 심각도 평가 ▲피해 유형 ▲사고 증빙 자료가 포함됨. 이를 통해 사고 기록의 표준화와 국가 간 호환성을 제고하고, 재발 방지 분석의 질을 높이려는 목적을 제시
- OECD는 해당 프레임워크가 국가 간 상호운용성을 높이고 정책결정자가 고위험 AI 시스템을 보다 신속하게 식별할 수 있도록 돕는 기반이 될 것이라고 평가함. 특히 사고가 발생한 후 대응하는 방식에서 벗어나, 사고 보고 데이터 기반의 장기 분석을 통해 사전적 위험 식별과 예방적 정책 설계가 가능해진다는 점을 강조

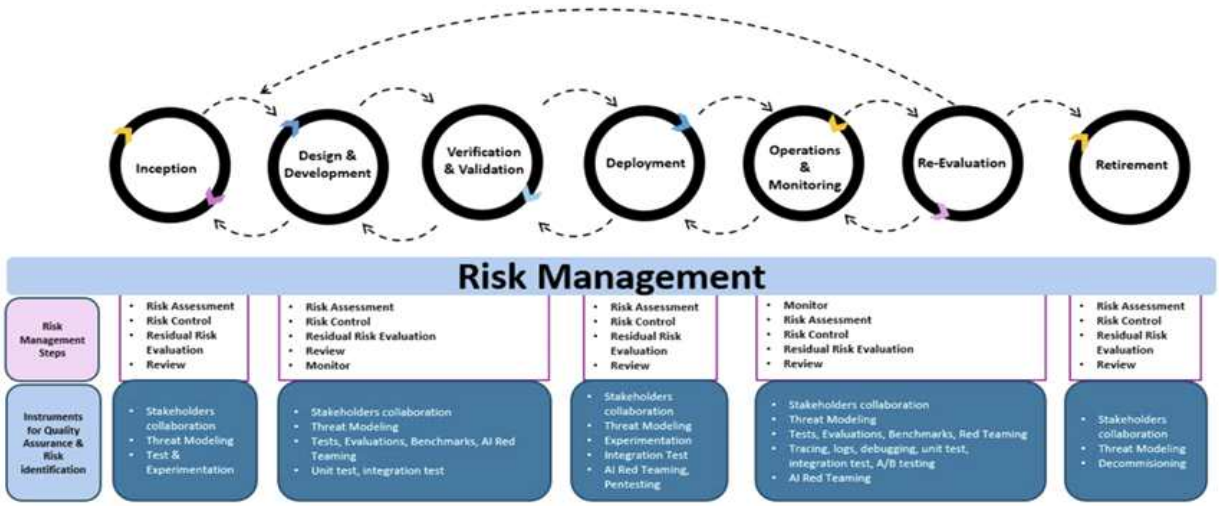
출처:
- International: OECD publishes report on common framework for AI incidents (DataGuidance, 2025.03.01.) https://www.DataGuidance.com/news/international-oecd-publishes-report-common-framework
- Towards a common reporting framework for AI incidents (OECD, 2025.02.28.) https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/02/towards-a-common-reporting-framework-for-ai-incidents_8c488fdb/f326d4ac-en.pdf

4월 EU: EDPB, LLM의 프라이버시 리스크 관리 프레임워크 보고서 발간

❖ 주요 내용

- 2025년 4월 10일, EU 개인정보보호이사회(European Data Protection Board, EDPB)는 거대언어모델(Large Language Model, LLM)의 프라이버시 위험을 식별·평가·완화하기 위해 「인공지능 프라이버시 위험 및 완화편(AI Privacy Risks & Mitigations – Large Language Models (LLMs)」 보고서를 발간함. 보고서는 LLM 확산에 따라 증가하는 프라이버시 위험을 생애주기 전반에서 관리하기 위한 기준을 제시
- 보고서는 LLM을 ▲서비스형(Service-based Model)* ▲상용 제품형(Commercial Product Model)** ▲자체 개발형(In-house Model)*** ▲에이전트 시스템형(Agent-based System)****으로 구분하고, 각 유형별 데이터 흐름을 바탕으로 발생 가능한 주요 프라이버시 위험을 제시함. 특히 이용자 입력·API 연동·모델 출력 과정에서 민감정보 노출, 비인가 접근, 데이터 오남용, 재식별 가능성 등이 공통 위험으로 나타남.

  * 서비스형(Service-based Model): 외부 제공자의 LLM API·클라우드 모델을 호출해 기능을 사용하는 방식의 구조.
  ** 상용 제품형(Commercial Product Model): 기업이 패키지 형태로 제공하는 사전 구축 LLM 제품을 그대로 도입해 활용하는 구조.
  ***자체 개발형(In-house Model): 조직이 자체 데이터·인프라를 기반으로 LLM을 직접 개발·학습·운영하는 구조.
  **** 에이전트 시스템형(Agent-based System): LLM이 외부 도구·시스템을 직접 호출하며 자율적 작업 수행이 가능한 구조.
- LLM 생애주기는 기획·설계부터 배포·운영·종료까지 8단계로 분류되며, EDPB는 각 단계에서 고려해야 할 프라이버시 위험 및 완화 조치를 제시함. 데이터 준비·학습 단계의 투명성 부족, 운영 단계의 모니터링 미흡, 업데이트 과정의 통제 어려움 등이 주요 위험으로 지적됨.



- 보고서는 GDPR과 「EU AI법(AI Act)」에 따라 컨트롤러·프로세서·공급자·배포자 등 LLM 관련 주체별 법적 책임을 제시하고, 특히 컨트롤러의 적법성 판단과 영향평가 실시 여부 결정, 정보주체 권리 보장 의무를 강조함. 이어 리스크 식별-평가-통제-모니터링으로 구성된 위험 관리 프레임워크를 통해 등급화와 완화·이전·회피·수용 등 처리 옵션을 안내하고, 각 단계의 절차와 메트릭을 간결히 제시함. 또한 챗봇 구현, 학습 분석 서비스, 여행·예약 플랫폼 등 사례를 통해 유형별 위험의 실제 적용 방식을 설명하며, LLM 기술의 급속한 발전에 대응하기 위해 위험 기반 접근과 규범 정비, 지속적 재평가·모니터링, 조직의 책임성 강화가 필요함을 강조함.

출처:
· EU: EDPB publishes report on AI Privacy Risks and LLMs (DataGuidance, 2025.04.10.)
https://www.DataGuidance.com/news/eu-edpb-publishes-report-ai-privacy-risks-and-llms
· AI Privacy Risks & Mitigations Large Language Models (LLMs)(EDPB, 2025.04.10.)
https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf

5월 ISO, AI 영향평가 기준 표준 발표

❖ 주요 내용

- 2025년 5월 28일, 국제표준화기구(International Organization for Standardization, ISO)와 국제전기표준회의(International Electrotechnical Commission, IEC)는 인공지능 시스템의 사회적·인간적 영향을 식별·평가하기 위한 국제표준 ISO/IEC 42005:2025를 공동 발표함. 본 표준은 AI 시스템의 설계 단계부터 운영·종료, 사후 모니터링에 이르기까지 전 생애주기에서 발생 가능한 영향을 구조적으로 관리할 수 있도록 절차를 제시
- ISO/IEC 42005는 AI 시스템 영향평가(AI System Impact Assessment)*를 조직이 수행하기 위한 핵심 프레임워크로 제시하며, 기존 국제표준과의 통합 가능성을 강조함. 특히 ISO/IEC 42001(AI 관리체계), ISO/IEC 23894(AI 위험관리), ISO/IEC 38507(AI 거버넌스), ISO/IEC 29134(개인정보 영향평가)와의 연계를 통해 하나의 일관된 AI 관리·감독 체계 구축이 가능하도록 설계됨.
  * AI 시스템 영향평가(AI System Impact Assessment): AI가 개인·사회에 미치는 의도된·비의도된 영향을 식별·평가·기록하는 절차.
- 주요 요구사항은 평가 절차의 문서화, 기존 관리시스템과의 정렬, 평가 시점 및 재평가 기준 설정, 책임자 지정, 민감한 사용 사례와 임계값 정의, 영향 분석 및 보고, 승인 절차 마련, 사후 모니터링 체계 구축 등으로 구성됨. 이러한 구성 요소는 AI 운영 과정의 투명성·책임성 확보를 위한 최소 요건으로 설명됨.
- 표준은 AI 시스템이 개인·집단·사회에 미칠 수 있는 긍정적·부정적 영향을 모두 고려하도록 요구하며, 데이터세트(dataset) 품질과 보안성, 알고리즘 특성, 배포 환경, 이용자·피이용자 등 이해관계자 범위, 예상 가능한 비의도된 영향 등을 필수 평가 항목으로 제시함. 또한 시스템 오작동·오남용·예측 불가한 상호작용 등 부정적 영향 가능성을 사전에 포착하는 것이 영향평가의 핵심이라고 강조
- ISO/IEC 42005는 부속자료(Annex)를 통해 영향 및 편익 분류체계(taxonomy), 기존 국제표준과의 정합성 안내, 평가 프로세스 흐름도, 영향평가 템플릿 등 실무 중심 도구를 제공함. 이러한 부속자료는 조직의 평가 수행 부담을 줄이고, 영향평가의 품질과 일관성을 유지하도록 지원하는 기능을 수행
- 보고서는 영향평가를 통해 조직이 공정성·안전성·인간 중심 설계라는 핵심 원칙을 구현할 수 있으며, AI 기술의 사회적 신뢰 확보와 규제 준수에도 중요한 기반이 된다고 설명함. ISO와 IEC는 기술 변화 속도에 대응해 영향평가 체계를 지속적으로 갱신할 것을 권고하며, 조직 내부의 위험관리·거버넌스 체계와의 통합적 운영을 강조

출처:
- International: ISO publishes AI impact assessment standard (DataGuidance, 2025.05.30.) https://www.DataGuidance.com/news/international-iso-publishes-ai-impact-assessment
- Technical Memorandum: What is new with the ISO/IEC 42005:2025 Standard for AI System Impact Assessment (SSRN, 2025.05.06.) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5191295

6월 프랑스: CNIL, AI 학습용 데이터 처리의 적법성 기준 권고안 발표

❖ 주요 내용

- 2025년 6월 19일, 프랑스 개인정보 감독기관(Commission nationale de l'informatique et des libertés, CNIL)은 AI 시스템 개발 과정에서 개인정보를 처리할 때 정당한 이익(legitimate interest)*을 법적 근거로 활용할 수 있는 조건을 제시한 권고안을 발표함. 이번 권고안은 2024년 공공 협의를 통해 수렴한 의견을 반영하여 마련된 것으로 AI 개발의 합법성·투명성 확보를 목표로 함.

  * 정당한 이익(Legitimate Interest): 개인정보 처리의 법적 근거 중 하나로, 조직이 추구하는 목적이 정보주체의 권리보다 우선할 수 있다고 인정되는 경우 적용 가능.

- CNIL은 AI 개발이 반드시 동의를 전제로 하지 않으며, 강력한 보호조치를 전제로 할 경우 정당한 이익을 개인정보 처리의 법적 근거로 인정할 수 있다고 명시함. 특히 데이터 수집·재사용 과정에서 정보주체 권리와 최소 수집 원칙을 철저히 준수해야 하며, 민감한 정보 또는 정보주체의 합리적 기대를 벗어나는 데이터 수집은 원칙적으로 금지됨.

- 이용자 대화 데이터(conversational data)를 AI 모델 개선 목적으로 재활용하는 경우, CNIL은 정보주체에 사전 통지를 실시하고, 가명처리(pseudonymization) 또는 익명처리를 적용하며, 처리 범위를 최소화하는 등 다층적 보호조치 마련을 요구함. 또한 정보주체에게 자유로운 반대권(right to object)을 제공해야 한다고 강조

- CNIL은 웹 스크래핑(web scraping)**을 통한 AI 학습용 데이터 수집에 대한 별도 기준도 제시함. 민감 정보가 포함되거나 아동이 주로 사용하는 사이트, 건강 관련 커뮤니티 등에서의 데이터 수집은 원칙적으로 금지되며, 스크래핑을 명시적으로 거부하는 웹사이트에 대한 수집도 허용되지 않음. 공개 데이터라 하더라도 목적·맥락·민감성 등을 고려하여 제한적으로 처리해야 한다고 명시

  ** 웹 스크래핑(Web Scraping): 웹사이트에서 자동화 도구를 사용해 데이터를 대량 수집하는 행위로, AI 학습 데이터 구축에 자주 활용

- 조직은 수집된 정보 중 불필요하거나 부적절한 데이터는 즉시 삭제해야 하며, 확인 즉시 식별 가능한 민감 정보는 처리 대상에서 제외해야 함. 또한 데이터 보존 정책을 명확히 설정하고, 재식별 위험을 최소화할 수 있는 기술적 관리적 보호조치를 마련해야 함.

- 본 권고안은 정당한 이익 기반 AI 개발에서 투명성·책임성 확보를 위한 기준을 제시하며, 모델 개발 초기 단계부터 개인정보 보호 요소를 설계에 반영할 것을 조직에 요구함. CNIL은 향후 AI 모델의 GDPR상 지위, 보안 요건, 데이터 주석(Annotation) 등에 대한 추가 권고도 발표할 예정

- CNIL은 또한 EU 개인정보보호이사회(European Data Protection Board, EDPB) 및 EU 집행위원회 AI 사무국과 협력하여 웹 스크래핑 규제, 생성형 AI의 데이터 처리 기준, 일반목적 AI(GPAI) 모범규약 등의 논의에도 지속적으로 참여할 계획

출처:
· Développement des systèmes d'IA : la CNIL publie ses recommandations sur l'intérêt légitime (CNIL, 2025.06.19.) https://www.cnil.fr/fr/recommandations-developpement-ia-interet-legitime
· France: CNIL publishes recommendations on AI and legitimate interest (DataGuidance, 2025.06.20.) https://www.DataGuidance.com/news/france-cnil-publishes-recommendations-ai-and

11월 EU: EDPS, 인공지능 시스템 위험관리 지침 발표

❖ 주요 내용

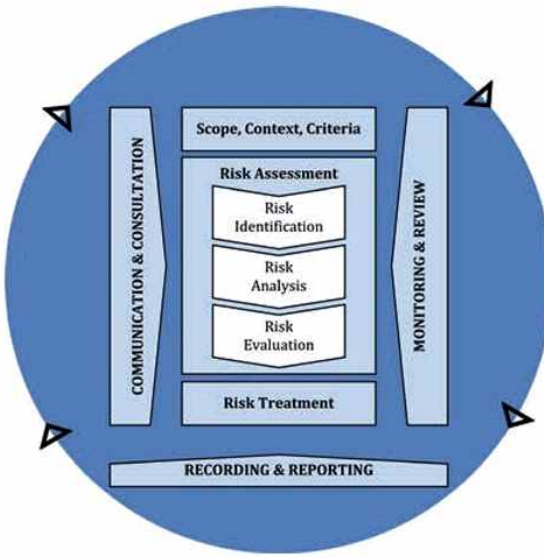
- 2025년 11월 11일, EU 개인정보 감독기관(European Data Protection Supervisor, EDPS)은 AI 활용 과정에서 개인정보 침해 요소를 식별·완화하기 위한 「인공지능 시스템 위험관리 지침(Guidance for Risk Management of Artificial Intelligence Systems)」을 공개함. 본 지침은 EU 공공부문 전체의 AI 활용 과정에서 적용되는 최소 기준을 제시
- EDPS는 리스크 기반 접근(Risk-Based Approach)*을 핵심 원칙으로 규정하며, 국제표준 ISO 31000:2018을 참조해 위험 평가-완화-모니터링 절차를 구조화하도록 요구함. 이는 AI가 초래할 수 있는 기본권 침해 위험을 사전에 식별하고 문서화하는 체계적 관리의 필요성을 강조

  * 리스크 기반 접근(Risk-Based Approach): 위협 가능성과 영향도를 기준으로 위험을 평가·관리하는 절차.

- 지침은 개인정보 보호 준수 공백이 반복적으로 나타나는 핵심 영역을 해석가능성·공정성·정확성·최소수집·보안으로 분류하고, 데이터 품질 점검, 바이어스 검출, 모델 검증·재학습 등 기술적 조치의 병행을 권고함. 특히 EDPS는 설명가능성 확보 도구로 LIME(Local Interpretable Model-Agnostic Explanations)**과 SHAP(Shapley Additive Explanations)*** 활용을 예시로 제시하며, 모델 구조·편향 요인·한계 등을 내부적으로 문서화할 것을 강조

  ** LIME: 개별 예측을 단순 모델로 근사해 설명 변수를 도출하는 설명가능성 기법.

  *** SHAP: 입력 변수가 예측에 기여한 정도를 셰플리 값으로 설명하는 기법.



- 또한 정보주체 권리 보장에 있어 수집 데이터 식별 불완전성, 삭제·정정 미이행 등의 실무 문제를 지적하며, 메타데이터 관리 강화, 데이터 검색 도구 개발, 머신 언러닝(machine unlearning)**** 적용 가능성 등을 보완책으로 제안

  **** 머신 언러닝(Machine Unlearning): 특정 데이터의 영향을 모델에서 제거하거나 최소화하는 기술.

- 운영 단계에서는 다중요소 인증(Multi-Factor Authentication, MFA)·역할 기반 접근통제(Role-Based Access Control, RBAC), 암호화, 패치관리, 재현성 확보를 위한 문서화 등 조직적·기술적 보호조치의 상시 적용이 요구됨. 학습데이터의 적정성 사전 검토와 모델 검증 절차 공개도 필수 요소로 포함됨.
- EDPS는 이번 지침이 EU 기관의 AI 활용 전 과정에서 일관된 개인정보 보호수준을 확보하기 위한 최소 기준이라고 밝히며, 향후 EU 차원의 통합 AI 위험관리 체계 구축 논의를 이어갈 계획

출처:
- EU: EDPS publishes guidance on risk management of AI systems (DataGuidance, 2025.11.13.) https://www.DataGuidance.com/news/eu-edps-publishes-guidance-risk-management-ai-systems
- Guidance for Risk Management of Artificial Intelligence systems (EDPS, 2025.11.11.) https://www.edps.europa.eu/system/files/2025-11/2025-11-11_ai_risks_management_guidance_en.pdf

2. 개인정보 보호 강화기술(PETs)

(1) EU: CJEU, 가명처리 관련 의견 발표

(2) 이스라엘: PPA, 개인정보 보호 강화 기술(PETs) 가이드 발행

(3) 영국: ICO, 익명처리 관련 신규 가이드라인 발표

(4) 양자내성암호(PQC) 주목

(5) OECD, AI 모델 신뢰성 제고를 위한 개인정보 보호 강화 기술(PETs) 보고서 발행

(6) APAC, 홍콩·마카오, 익명화 시작을 위한 가이드 발간

(7) 개인정보위, '가명정보 제도·운영 혁신방안' 발표

2월 EU: CJEU, 가명처리 관련 의견 발표

❖ 주요 내용

- 2025년 2월 6일, EU 사법재판소(Court of Justice of the European Union, CJEU) 법무관 슈필만(Spielmann)은 EU 개인정보 감독기관(European Data Protection Supervisor, EDPS)와 단일해결위원회(Single Resolution Board, SRB) 간 분쟁(C-413/23)에 대한 의견을 제시함. 본 사건은 SRB가 외부 기관에 가명처리된 데이터를 제공하는 과정에서 정보주체 고지 의무를 충족했는지를 중심으로 쟁점이 형성됨.
- 사건의 배경은 SRB가 특정 절차 수행 과정에서 의견 제출자의 데이터를 가명처리(Pseudonymization)하여 공유하였으나, 가명처리에 사용된 식별 코드를 함께 전달해 정보주체 식별 가능성이 남아 있었다는 점에서 비롯됨. EDPS는 해당 데이터가 개인정보에 해당하며, 정보주체에게 데이터 전송 사실을 알릴 의무가 있었다고 주장
- 법무관은 규정(EU) 2018/1725 제3조(6)를 근거로 가명처리가 개인정보의 정의에 포함되는 개념은 아니라는 해석을 제시함. 가명정보(Pseudonymized Data)가 개인정보에 해당하는지 여부는 실질적 식별 가능성의 존재 여부를 기준으로 판단되어야 하며, 식별 가능성이 “완전히 배제되거나 극히 미미한 경우”에만 개인정보에서 제외될 수 있다고 판단함. 이는 EDPS의 폭넓은 적용 해석에 대해 제한적 기준을 명확히 제시한 것으로 평가됨.
- 다만 정보 제공 의무(Information Provision Duty)와 관련해서는 SRB의 책임을 인정함. 법무관은 규정(EU) 2018/1725 제4조와 제15조를 근거로 데이터가 이후 수신자의 관점에서 개인정보로 보이지 않을 가능성이 있더라도, 데이터 수집 단계에서 정보주체에게 처리 목적과 수신자를 알릴 의무가 존재한다는 점을 강조함. 따라서 데이터 전송 당시 가명처리의 견고성(Robustness)과 무관하게 투명성 확보 의무가 우선 적용된다는 해석을 제시
- 법무관 의견은 가명정보의 법적 지위가 단순히 기술적 처리 여부가 아니라 실질적 식별 위험 수준에 의해 결정됨을 재확인함과 동시에, 정보주체의 권리 보장을 위한 사전 고지의 필요성을 강화하는 방향성을 제시함. 본 의견은 향후 유럽연합 내 가명처리 활용 기준과 정보 제공 의무 해석에 영향을 미칠 가능성이 존재

출처:
- CJEU publishes AG Opinion on pseudonymization (DataGuidance, 2025.02.07.) https://www.DataGuidance.com/news/eu-cjeu-publishes-ag-opinion-pseudonymization
- OPINION OF ADVOCATE GENERAL SPIELMANN (CJEU, 2025.02.06.) https://curia.europa.eu/juris/document/document.jsf?text=&docid=295078&pageIndex=0&doclang=EN

2월 이스라엘: PPA, 개인정보보호 강화기술(PETs) 가이드 발행

❖ 주요 내용

- 2025년 2월 23일, 이스라엘 개인정보 감독기관(Privacy Protection Authority, PPA)은 개인정보 보호 강화기술(Privacy-Enhancing Technologies, PETs)의 이해와 적용을 지원하기 위한 실무 가이드를 발표함. 본 가이드는 개인정보보호책임자, 법률 자문, 제품·프로젝트 관리자 등을 대상으로 정보시스템 및 소프트웨어 설계 단계부터 PETs을 통합하기 위한 기준과 활용 사례를 제시
- PPA는 PETs을 개인정보 보호를 강화하는 기술적·관리적 접근법으로 정의하고, 데이터 사용 목적 달성을 지원하면서도 정보주체 권리 침해 위험을 최소화하는 기술군으로 설명함. 가이드에는 PETs의 적용 영역을 정보 준비 단계, 정보 사용 단계, 정보 사용 통제 단계로 구분하여 실무자가 시스템 전 생애주기에 PETs을 조직적으로 적용할 수 있도록 구조화
- 정보 준비 단계에서는 익명화(Anonymization), 데이터 최소화, 데이터 세분화 축소 등 식별 가능성을 낮추는 조치를 제시함. 합성데이터(Synthetic Data) 생성, 차등 프라이버시(Differential Privacy)* 적용 등 개인정보 노출을 억제하면서 분석 품질을 유지하는 기술도 주요 수단으로 포함됨.

  * 차등 프라이버시(Differential Privacy): 데이터 분석 과정에서 노이즈를 추가해 개별 정보 노출을 방지하는 기술.
- 정보 사용 단계에서는 원본 정보를 직접 노출하지 않고 연산을 수행할 수 있도록 하는 동형암호화(Homomorphic Encryption)**, 연합학습(Federated Learning)***, 다자간 연산(Multi-Party Computation, MPC)**** 등 분산형·암호 기반 기술을 제시함. 또한 특정 정보를 밝히지 않고도 진위를 증명할 수 있는 영지식증명(Zero-Knowledge Proofs)을 통해 정보 접근 최소화 원칙을 구현할 수 있음을 설명

  ** 동형암호화(Homomorphic Encryption): 암호화된 상태에서 연산 수행을 가능하게 해 원본 정보 노출을 방지하는 기술.
  *** 연합학습(Federated Learning): 데이터를 중앙 서버로 전송하지 않고 로컬 환경에서 머신러닝 모델을 학습하는 방식.
  **** 다자간 연산(MPC): 여러 참여자가 데이터를 공유하지 않고 공동 연산을 수행할 수 있도록 하는 기술.
- 정보 사용 통제 단계에서는 접근권한 관리, 정책 기반 통제, 사용 기록 추적 등을 포함해 정보주체가 자신의 정보 사용에 대한 통제력을 높일 수 있는 체계를 제시함. 가이드라인은 PETs의 도입이 「개인정보보호법(Protection of Privacy Law, PPL)」 준수와 데이터 활용 간 균형을 제공하며, 조직이 데이터 처리 과정에서 윤리적·법적 위험을 줄이는 데 기여한다고 평가
- PPA는 PETs이 글로벌 규제 환경에서 핵심적 개인정보 보호 전략으로 자리 잡고 있으며, 조직의 데이터 처리 투명성·책임성을 강화하는 기반 기술로 기능한다고 설명함. 또한 PETs이 기술적 보호조치를 넘어 조직의 개인정보 처리 문화 전반을 개선하는 방향으로 작동해야 한다고 강조

출처:
- Israel : PPA publishes guide on PETs (DataGuidance, 2025.02.24.)
  https://www.DataGuidance.com/news/israel-ppa-publishes-guide-PETs
- מדריך PETs לטכנולוגיות מגבירות-פרטיות (Israel PPA, 2025.02.23.)
  https://www.gov.il/he/pages/guide_enhancing_technologies?utm_source=go.gov.il&utm_medium=referral

3월 영국: ICO, 익명처리 관련 신규 가이드라인 발표

❖ 주요 내용

- 2025년 3월, 영국 개인정보 감독기관(Information Commissioner's Office, ICO)은 「익명처리 가이드라인(Anonymisation Guidance)」을 발표함. 본 가이드라인은 개인정보와 익명정보의 구분 기준과 함께, 조직이 효과적으로 익명처리를 수행하기 위한 절차와 원칙을 제시
- 가이드는 익명처리의 핵심 개념으로 일반화(generalisation)와 무작위화(randomisation)를 제시함. 일반화는 데이터 정밀도를 낮추어 식별 가능성을 줄이는 방법으로 연령대·지역 범주화 등 예시를 제시함. 무작위화는 노이즈 추가·값 변형·합성데이터(Synthetic Data) 생성 등을 통해 개별 기록과 실제 개인 간의 직접 연결을 약화하는 방식으로 설명됨.
- ICO는 익명처리와 가명처리(pseudonymisation)를 명확히 구분함. 해시·암호화·토큰화 등 가명처리 기법은 여전히 추가 정보를 통해 개인 식별이 가능한 개인정보로 간주되며, GDPR을 포함한 관련 규제 적용 대상임을 재확인함. 반면 익명처리는 합리적으로 식별 가능성이 없는 수준까지 위험을 낮춘 경우에만 인정됨.
- 식별성 판단 기준으로는 단일 식별(singling out)*과 연계 가능성(linkability)**을 제시함. 단일 식별은 동일 개인에 대한 기록을 고립·구분할 수 있는지 여부를 의미하며, 연계 가능성은 다른 데이터세트와 결합해 개인을 식별할 수 있는지 여부를 의미함. ICO는 이 두 요소를 고려한 위험 평가와 그 결과에 대한 문서화를 요구

  * 단일 식별(Singling Out): 데이터세트에서 특정 개인에 관한 기록을 다른 기록과 구분해 고립시킬 수 있는 상태.
  ** 연계 가능성(Linkability): 여러 데이터세트를 결합하여 동일 개인·집단에 관한 정보를 연결할 수 있는 가능성.
- 또한 ICO는 정보가 누구 손에 있는지에 따라 개인정보 여부가 달라질 수 있다는 '정보 소유자(whose hands)' 테스트***를 도입함. 이는 특정 조직이 합리적으로 이용 가능한 수단을 통해 개인을 식별할 수 있는지 여부를 기준으로 정보의 법적 성격을 판단하는 방식으로, 공표가 아닌 제3자 간 제공 상황에서 특히 중요하다고 설명

  *** 정보 소유자 테스트(Whose Hands Test): 정보가 놓인 주체가 합리적으로 이용 가능한 수단을 통해 개인을 식별할 수 있는지 여부에 따라 개인정보 여부를 판단하는 기준.
- 가이드라인은 익명처리가 일회성 조치가 아니라는 점도 강조함. 기술 발전, 외부 데이터 공개, 양자컴퓨터 등 환경 변화에 따라 익명처리의 효과가 저하될 수 있으므로, 정기적인 식별 위험 재평가와 의욕적 침입자 테스트(motivated intruder test)**** 수행, 추가 정보의 안전한 삭제, 공개 범위·수신자 그룹에 따른 차등적 보호조치 설계 등 거버넌스 체계 마련이 필요하다고 제시

  **** 의욕적 침입자 테스트(Motivated Intruder Test): 합리적 능력과 자원을 가진 외부인이 재식별을 시도하는 상황을 가정해 익명처리의 효과를 점검하는 평가 방법.

출처:
- UK: The ICO's new guidance on anonymization – part one (DataGuidance, 2025.06.14.) https://www.dataguidance.com/opinion/uk-icos-new-guidance-anonymization-part-one
- UK: The ICO's new guidance on anonymization – part two (DataGuidance, 2025.06.14.) https://www.DataGuidance.com/opinion/uk-icos-new-guidance-anonymization-part-two
- Anonymisation (ICO, 2025.03.28.) https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/anonymisation/

4월 양자내성암호(PQC) 주목

❖ 주요 내용

- 양자컴퓨터 기술 발전으로 기존 공개키 암호체계의 무력화 가능성이 제기되면서, 양자내성암호(Post-Quantum Cryptography, PQC)*가 차세대 암호 기술로 빠르게 부상함.

  * 양자내성암호(PQC): 양자컴퓨터로도 현실적인 시간 안에 해독하기 어려운 수학적 문제를 기반으로 설계된 차세대 암호 기술.

- 현재 널리 사용되는 RSA 암호**와 같은 기존 공개키 암호는 쇼어 알고리즘을 활용한 양자컴퓨터의 대규모 연산 능력 앞에서 2030년대 이후 서서히 취약해질 수 있다는 우려가 제기됨. 이에 따라 격자 기반 암호(Lattice-Based Cryptography)***, 해시 기반 암호, 다변수 다항식 기반 암호 등 다양한 PQC 연구·표준화가 병행되는 상황

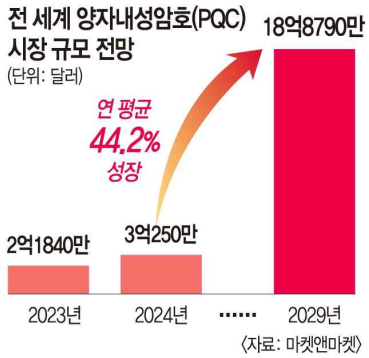
  ** RSA 암호(RSA Encryption): 큰 소수의 곱셈과 소인수분해의 어려움을 이용해 보안성을 확보하는 대표적 공개키 기반 비대칭 암호 알고리즘.

  *** 격자 기반 암호(Lattice-Based Cryptography): 고차원 격자 구조의 수학적 난제를 이용해 양자컴퓨터 시대에도 높은 보안성을 제공하도록 설계된 양자내성암호 기법.

- 국내에서는 2023년 국가정보원과 과학기술정보통신부가 공동으로 범국가 PQC 전환 마스터플랜을 수립하고 2035년까지 국가 암호체계를 단계적으로 PQC로 전환할 계획을 제시함. 이후 한국인터넷진흥원(KISA) 주관 한국형 PQC 공모전을 통해 격자 기반 전자서명 알고리즘 등 국산 알고리즘을 선정·검증하는 작업이 진행됨.

- 2025년에는 에너지·의료·행정 분야 정보통신 인프라를 대상으로 PQC 시범전환 지원사업이 본격 추진됨. 전력 사용량 원격 검침 시스템, 의료 데이터 중계 플랫폼, 국가기술자격검정 시스템 등 국민 생활과 밀접한 인프라에서 암호체계를 PQC로 전환해 실증하는 것을 목표로 함. 이후 통신·국방·금융·우주·환경·사물인터넷 등으로 전환 대상을 확대하는 단계적 로드맵도 병행됨

- 민간 기업의 기술 적용도 빠르게 확산되는 중임. LG유플러스(LG Uplus)는 PQC 기반 계정관리 솔루션과 가상 사설망(Virtual Private Network, VPN) 서비스를 상용화했으며, 삼성SDS(Samsung SDS)는 한국과학기술원(KAIST)과 공동 개발한 전자서명 알고리즘 'AIMer'를 PQC 국가공모전 최종 알고리즘으로 선정시키는 성과를 확보함.



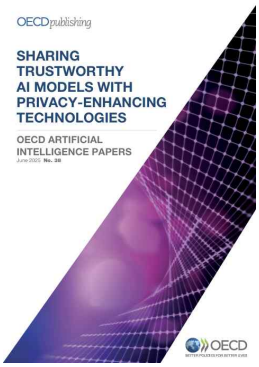
〈자료: 마켓앤마켓〉

- 다만 PQC 도입이 가속화될수록 기존 시스템과의 호환성 문제, 암호키 관리, 성능 저하, 구현 오류 등 새로운 보안·운영 리스크도 동반됨. 특히 국가·산업 인프라에 저장된 민감한 개인정보와 기업 기밀을 보호하는 과정에서, PQC 전환과 개인정보 보호 체계 강화를 병행하는 전략 수립이 필요한 상황

출처:
- 양자컴도 못 뚫는 '양자내성암호'…에너지·의료·행정 인프라 최초 적용 (뉴시스, 2025.04.14.) https://n.news.naver.com/article/003/0013181167?sid=105
- '양자기술로 안뚫리는 국가암호'…정부, 시범사업 착수 (아시아경제, 2025.03.17.) https://n.news.naver.com/mnews/article/277/0005561838?sid=105
- 업계 주목받는 양자내성암호…"양자컴 해킹 공격 막고 데이터 보호" (국민일보, 2025.03.12.) https://n.news.naver.com/mnews/article/005/0001762469?sid=101

6월 OECD, AI 모델 신뢰성 제고를 위한 개인정보보호 강화 기술(PETs) 보고서 발행

❖ 주요 내용



- 2025년 6월 17일, 경제협력개발기구(Organisation for Economic Co-operation and Development, OECD)는 「신뢰성 있는 인공지능 모델 공유를 위한 개인정보보호 강화 기술 활용 보고서(SHARING TRUSTWORTHY AI MODELS WITH PRIVACY-ENHANCING TECHNOLOGIES)」를 발간하며 AI 모델 개발·공유 과정에서 개인정보 보호와 기밀성 확보를 위한 기술·정책 프레임워크를 제시함. 생성형 인공지능 확산으로 개인정보 및 민감정보 보호 문제가 고도화되는 가운데, PETs는 데이터 최소 처리와 안전한 공동 개발을 지원하는 핵심 기술로 부상
- 보고서는 2024년 OECD PETs-AI 전문가 워크숍 논의를 기반으로 PETs 활용 사례 유형(use case archetype)을 체계화함. 첫째, 입력·테스트 데이터 최소화를 위한 기술로 신뢰 실행 환경(Trusted Execution Environment, TEE)*, 차등 프라이버시(Differential Privacy), 연합 학습(Federated Learning) 등이 제시됨. TEE는 운영체제 외부에서 민감 데이터를 격리·보호하며 연산을 수행하는 보안 하드웨어 영역을 의미함. 둘째, 모델 공동 개발 및 공유 단계에서 활용 가능한 기술로 동형 암호화(Homomorphic Encryption), 합성데이터(Synthetic Data), 다자간 연산(Multi-Party Computation, MPC)**, 사적 집합 교차(Private Set Intersection, PSI)*** 등이 포함됨. 이러한 기술 조합은 기밀성 유지와 데이터 접근 최소화를 동시에 충족하는 환경 조성에 기여

  * 신뢰 실행 환경(TEE): 운영체제와 분리된 보안 하드웨어 영역에서 민감 데이터를 보호하며 연산을 수행하는 환경.
  ** 다자간 연산(MPC): 데이터를 직접 공유하지 않은 채 여러 주체가 연산을 수행할 수 있도록 하는 암호 기술.
  *** 사적 집합 교차(PSI): 참여자가 각자의 데이터세트를 공개하지 않고 공통 원소만을 안전하게 도출하는 암호 프로토콜.
- OECD는 PETs가 데이터 접근·공유에 관한 OECD 권고(Recommendation of the Council on Enhancing Access to and Sharing of Data)의 목표와 부합한다고 평가함. 다만 PETs는 단독 사용 시 정확성·효율성·사용성 간 균형 확보가 어렵고, 연산 비용 및 통신 부하 증가 등 기술적 제약이 존재함. 예컨대 차등 프라이버시와 합성데이터는 모델 정확도 저하 가능성이 있으며, 동형 암호화와 MPC는 높은 연산 자원 소모가 수반됨. 연합 학습 역시 업데이트 경로를 통한 정보 유출 위험이 존재
- 정책 측면에서 OECD는 PETs 채택 촉진을 위해 수요자 중심 정책(규제 샌드박스, 공공 조달)과 공급자 중심 정책(R&D 지원, 기술 가용성 확대)을 병행해야 함을 강조함. 싱가포르·영국·노르웨이 등은 규제 샌드박스 운영, 공동 경진대회 개최, 산학 협력, 공공 조달 프로그램 등을 통해 PETs 실증과 기술 확산을 지원 중임. 또한 중소기업의 도입 장벽을 완화하기 위한 국가 차원의 지원 전략 필요성도 제기됨.
- 보고서는 PETs가 기술 발전과 개인정보 보호 간 균형을 확보하는 핵심 도구라는 점을 강조하며, 사례 기반 표준화와 국가 간 규제 조화가 데이터 거버넌스 정합성 제고로 이어질 수 있다고 분석함. OECD는 향후 PETs 국제 비교 사례집 구축과 기술 발전에 대응하는 유연한 정책 설계를 권고

출처:
- International: OECD publishes report on sharing trustworthy AI models with privacy-enhancing technologies (DataGuidance, 2025.06.18.) https://www.DataGuidance.com/news/international-oecd-publishes-report-sharing
- Sharing trustworthy AI models with privacy-enhancing technologies (OECD, 2025.6.17.) https://www.oecd.org/en/publications/sharing-trustworthy-ai-models-with-privacy-enhancing-technologies_a266160b-en.html

7월 APAC, 홍콩·마카오, 익명화 시작을 위한 가이드 발간

❖ 주요 내용

- 2025년 7월 31일, 홍콩 개인정보 감독기관(Office of the Privacy Commissioner for Personal Data, PCPD)과 마카오 개인정보 감독기관(Personal Data Protection Bureau, PDPB)이 공동으로 「익명처리 시작 가이드(The Guide to Getting Started with Anonymisation)」를 발간함. 본 가이드는 아시아태평양 개인정보보호감독기구(Asia Pacific Privacy Authorities, APPA) 소속 7개 감독기구의 승인을 거쳐 마련된 지역 공동 지침으로, 조직의 데이터 활용 과정에서 재식별 위험을 최소화하기 위한 절차적 기준을 제시
- 가이드는 익명처리(Anonymisation) 수행 단계를 ① 데이터 파악, ② 직접 식별자(Direct Identifier)* 제거, ③ 익명처리 기술 적용, ④ 재식별 위험 평가, ⑤ 잔여 위험 관리의 5단계 프로세스로 구조화함. 먼저 데이터 유형을 직접 식별자와 간접 식별자(Indirect Identifier)**로 구분하여 식별 가능성을 진단하도록 규정하며, 이후 데이터 마스킹·범주화·값 치환 등 익명처리 기법 적용 절차를 제시함. 특히 익명처리 후에도 데이터세트 내 재식별 가능성이 남아 있는 경우 해당 데이터는 여전히 개인정보로 간주됨을 명확히 하며, GDPR·각국 개인정보보호법과 동일한 규제 적용 대상으로 해석
  * 직접 식별자(Direct Identifier): 이름, 주민등록번호 등 단독으로 개인을 식별할 수 있는 정보.
  ** 간접 식별자(Indirect Identifier): 단독으로는 식별이 불가능하나 결합 시 개인 식별이 가능한 정보.
- 또한 본 가이드는 국제표준 ISO/IEC 27559(익명처리 프레임워크) 및 ISO/IEC 20889(개인정보보호 강화기술)과의 정합성을 강조하며, 실무 적용 시 참고 가능한 국제적 기준과의 연계를 확보함. 더불어 외부 공격자가 재식별을 시도하는 상황을 가정한 의욕적 침입자 테스트(Motivated Intruder Test)***를 포함하여 기술적 조치뿐 아니라 법적·관리적 대응의 병행 필요성을 강조
  *** 의욕적 침입자 테스트(Motivated Intruder Test): 외부인이 합리적으로 접근 가능한 정보와 자원을 활용해 재식별 시도를 하는 상황을 가정한 위험 평가 방법.
- APPA 기술작업반 주도로 한국 개인정보보호위원회(Personal Information Protection Commission, PIPC), 일본 개인정보 감독기관(Personal Information Protection Commission, PPC), 싱가포르 개인정보 감독기관(Personal Data Protection Commission, PDPC) 등이 참여해 공동 개발한 가이드로, 향후 역내 데이터 거버넌스 정합성 제고에 기여할 전망임. PCPD는 가이드에서 제시된 절차가 공공·민간 조직의 익명처리 책임성 및 규제 준수 수준을 강화할 수 있는 실무 기준이라고 설명

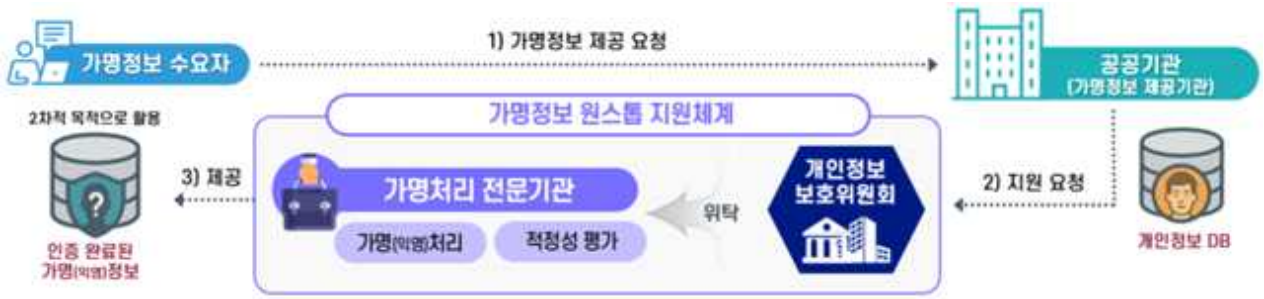
출처:
- APAC: Hong Kong and Macau releases the guide to getting started with anonymization (DataGuidance, 2025.08.01.) https://www.DataGuidance.com/news/apac-hong-kong-and-macau-releases-guide-getting
- Guide to Getting Started with Anonymisation (PCPD, 2025.07.31.) https://www.pcpd.org.hk/english/resources_centre/publications/files/appa_anonymisation_guide072025.pdf

9월 개인정보위, '가명정보 제도·운영 혁신방안' 발표

❖ 주요 내용

- 2025년 9월 24일, 개인정보위는 「가명정보 제도·운영 혁신방안」을 발표하며 공공부문의 가명정보 활용 기반을 대폭 확장하는 정책 방향을 제시함. 핵심 목표는 공공기관의 가명정보 활용 비율을 2027년까지 50%로 높이고, 데이터 제공 기간을 기존 평균 310일에서 100일 이내로 단축
- 혁신방안에는 전문기관을 통한 가명처리 원스톱 서비스 도입이 포함되며, 공공기관의 법적 부담을 완화하고 절차적 효율성을 확보하는 구조 마련이 추진됨. 아울러 연내 가명정보 비조치 의견서(No Action Letter) 제도*를 신설하여 법 적용의 불확실성을 해소하고 개별 사안별 판단 기준을 제공함.

  * 비조치 의견서(No Action Letter): 특정 데이터 처리 행위에 대해 규제기관이 행정조치 대상 여부를 사전에 통지하는 제도.



- 또한 개인정보위는 「가명정보 처리 가이드라인」 개정을 통해 데이터 위험도**와 처리환경 취약도에 따른 차등 심의 체계를 구축함. 위험도가 낮은 경우 서면심의로 대체하는 방식이며, 이미지·영상 등 비정형 데이터는 표본조사 기반의 가명처리 적정성 검토를 허용하는 등 대규모 데이터 활용 환경의 현실성을 반영한 절차 간소화가 이루어짐.

  ** 데이터 위험도(Data Risk Level): 재식별 가능성과 피해 규모 등을 고려해 데이터 처리 위험성을 평가하는 지표.
- 이어 2025년 11월 5일, 개인정보위는 「가명정보 비조치 의견서」 제도의 시범 운영을 개시함. 본 제도는 가명정보 처리 과정에서 법령 위반 여부를 사전에 확인할 수 있는 공식 채널로, 신청인은 구체적 처리 행위를 제출하고 개인정보위는 30일 이내 행정조치 대상 여부를 회신함. 회신 내용은 온라인 플랫폼을 통해 공개되어 시장 전반의 예측 가능성을 높이는 기능을 수행
- 비조치 의견서는 기업·연구기관의 위축 요인을 해소하고 적법한 가명처리를 지원하는 것을 주된 목적으로 하며, 기존 금융권의 비조치의견 제도를 벤치마킹한 형태임. 개인정보위는 시범운영 결과를 바탕으로 2026년 관련 법적 근거를 마련할 계획
- 이번 정책 발표는 공공·민간 영역에서 가명정보 활용도를 확대함과 동시에, 절차 합리화와 규제 명확화를 기반으로 데이터 기반 산업 경쟁력 제고를 도모하는 정책적 의미를 가짐. AI 시대 고품질 데이터 확보와 개인정보 보호의 균형을 위한 제도적 기반 강화라는 점에서 향후 데이터 거버넌스 체계 전반에 실질적 영향을 미칠 전망

출처:
- 개인정보위 가명정보 제도 운영 혁신방안 발표 (디지털타임스, 2025.09.24.) https://n.news.naver.com/mnews/article/029/0002984117?sid=105
- 개인정보위, "'가명정보' 활용 전 법령 위반 여부 확인하세요" (디지털타임스, 2025.11.05.) https://n.news.naver.com/mnews/article/029/0002991559?sid=105
- 가명정보 활용 문턱 낮추고, 데이터 혁신 촉진한다 (개인정보위, 2025.09.24.) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=11504

3. 생체인식 기술·디지털 신원

(1) 중국: TC260, 얼굴 인식 결제의 개인정보 보호 요구사항 가이드 발행

(2) 중국: CAC, 얼굴인식 기술 보안에 관한 규정 발효

(3) 멕시코: 전 국민 대상 생체정보 등록 의무화 결정

(4) 미국: NIST, 개정된 디지털 신원 지침 발간

(5) 캐나다: OPC, 생체인식 관련 지침 발표

(6) 미국: EPIC, ICE에 얼굴인식기술 사용 중단 촉구

1월 중국: TC260, 얼굴 인식 결제의 개인정보 보호 요구사항 가이드 발행

❖ 주요 내용

- 중국 국가정보보안표준화기술위원회(National Information Security Standardization Technical Committee, TC260)는 2025년 1월 26일 「사이버보안 표준 실천 가이드-얼굴 인식 결제 시나리오 개인정보보호 요구사항(Cybersecurity Standard Practice Guide – Personal Information Security Protection Requirements in Facial Recognition Payment Scenarios)」을 발간함. 본 가이드는 얼굴 인식 결제 서비스 제공자, 얼굴 인증 서비스 제공자, 장소 관리자, 장비 운영자를 대상으로 데이터 수집·저장·전송·삭제 등 전주기 보호 기준을 제시
- 가이드는 장비 운영자와 장소 관리자가 얼굴 인식 결제 과정에서 생성된 개인정보를 처리해서는 안 된다고 규정하며, 서비스 제공자는 개인정보 영향평가(Personal Information Protection Impact Assessment, PIPIA)를 사전에 수행해야 함. 얼굴 인증은 개인의 명시적 동의 확보 후에만 진행 가능하며, 동의 문구에는 기술 사용의 필요성과 이용자 권익 영향이 포함되어야 함.
- 데이터 수집 단계에서는 최소 이미지 원칙, 이용자 능동적 참여 기반 수집, 비동의 수집분의 즉시 삭제 의무 등이 요구됨. 저장 단계에서는 복원 불가능한 얼굴 특성 템플릿만 저장하고, 기타 데이터는 금지되며, 물리·논리적 분리, 암호화 저장 등 강화 조치를 요구
- 전송 단계에서는 불가역·비연결성 특성을 충족한 데이터만 전송 가능하며, 양방향 인증·무결성 검증·암호화 전송을 의무화함. 외부 제공 시에는 별도 PIPIA 수행 및 적법한 근거 확보가 필요함. 삭제 단계에서는 처리 목적 달성 즉시 전 과정 데이터를 삭제하고, 삭제·익명처리의 비복원성(Non-reversibility)* 검증을 요구

  * 비복원성(Non-reversibility): 저장된 얼굴 특성이 원본 이미지로 재구성될 수 없도록 보장하는 성질.
- 장소 관리자와 장비 운영자는 카메라 비정상 작동 방지, 촬영 구역 제한, 이용자 오인 방지 표시, 비필요 카메라 비활성화, 얼굴 인식 결제 비기본값 설정 등 추가 보호조치를 준수해야 함. 특히 운영 장비는 얼굴 촬영을 필수 선택지로 강제해서는 안 되며, 이용자에게 대체 결제수단을 동등하게 제공해야 함.
- 이번 가이드는 얼굴 인식 결제 생태계 전체를 규율하는 기술·관리적 기준을 통합적으로 제시함으로써 「개인정보보호법(Personal Information Protection Law, PIPL)」, 「데이터보안법(Data Security Law)」 등 중국 법제와 연계된 실무적 준거 틀을 제공했다는 점에서 의의가 있음.

출처:
- China: TC260 publishes guide on personal information security requirements in facial recognition payments (DataGuidance, 2025.01.27.) https://www.DataGuidance.com/news/china-tc260-publishes-guide-personal-information
- 网络安全标准实践指南 (TC260, 2025.01.26.) https://www.tc260.org.cn/upload/2025-01-26/1737864764732021867.pdf

6월 중국: CAC, 얼굴인식 기술 보안에 관한 규정 발효

❖ 주요 내용

- 2025년 6월 1일, 중국 국가인터넷정보판공실(Cyberspace Administration of China, CAC)과 중화인민공화국 공안부(Ministry of Public Security, MPS)가 공동 제정한 「얼굴인식 기술 응용 안전관리 조치(人脸识别技术应用安全管理办法)」가 시행됨. 본 조치는 연구·개발 목적을 제외한 모든 얼굴인식기술(Facial Recognition Technology, FRT) 활용을 규율하여 개인정보 처리의 요건과 보안 기준을 명문화
- 개인정보처리자는 처리 목적·방식·영향·권리 행사 절차 등을 정보주체에게 명확히 고지할 의무를 부담하며, 고지 내용이 변경될 경우 재고지 의무가 발생함. 동의를 법적 근거로 하는 경우 자발적이고 명시적인 단독 동의를 사전에 확보해야 하며, 만 14세 미만 미성년자의 경우 보호자 동의 확보가 요구됨. 정보주체는 언제든지 동의를 철회할 수 있으며, 철회 전 처리의 효력은 유효로 간주
- 얼굴정보는 원칙적으로 기기 내부 저장이 요구되며, 인터넷 외부 전송은 금지됨. 처리 대상이 10만 명 이상에 이르면 개인정보처리자는 30영업일 이내에 관할 성(省)급 이상 인터넷정보당국에 신고해야 하며, 이후 변동사항 발생 시 동일 기한 내 변경 신고의무가 부과됨.
- 신원 확인에 얼굴인식을 사용하는 경우 반드시 대체 인증수단을 병행 제공해야 하며, 이용자에게 얼굴정보 제공을 강요하거나 기망·오도하는 행위는 금지됨. 공공장소에서 얼굴인식 기기를 설치하는 경우 공공안전 목적의 필요성이 인정되어야 하며, 합리적인 촬영 구역 설정 및 경고 표식 설치가 요구됨.
- 보안조치 측면에서 본 조치는 암호화, 접근통제, 권한관리, 침입탐지 등 기술적 보호조치를 의무화함. 위반 시 「개인정보보호법(Personal Information Protection Law, PIPL)」, 「데이터 보안법(Data Security Law)」 등 관계 법령에 따른 제재가 적용됨. 누구든지 위법한 얼굴인식 정보 처리에 대해 신고할 수 있으며, 당국은 신고 처리 및 통지 의무를 부담
- 본 조치는 얼굴정보를 포함한 민감정보 처리의 오·남용을 방지하기 위한 규제체계로서, 중국 내 생체 정보 보호 강화 흐름을 제도적으로 구체화한 조치로 평가됨.

출처:
- China: Measures on security of facial recognition technology enter into force (DataGuidance, 2025.06.02.) https://www.DataGuidance.com/news/china-measures-security-facial-recognition-technology
- 关于开展人脸识别技术应用备案工作的公告 (CAC, 2025.05.30.) https://www.cac.gov.cn/2025-05/30/c%5F1750315544241157.htm
- 人脸识别技术应用安全管理办法 (CAC, 2025.03.21.) https://www.cac.gov.cn/2025-03/21/c_1744174262156094 6.htm

7월 멕시코: 전 국민 대상 생체정보 등록 의무화 결정

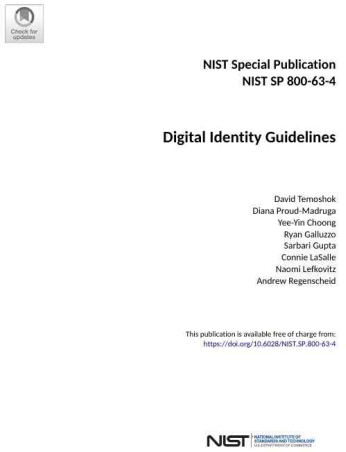
❖ 주요 내용

- 2025년 7월, 멕시코 정부는 기존 선택 사항이던 인구등록번호(Clave Única de Registro de Población, CURP)*를 생체정보 기반 의무 신분증으로 전환하는 개정안을 공포함. 새 CURP에는 이름·생년월일·성별·국적 등 기존 정보 외에 지문·홍채·안면 사진과 QR 코드 기반 생체정보가 포함되며, 2026년 2월까지 전 국민을 대상으로 단계적 발급이 진행될 예정임.
  * 인구등록번호 (CURP): 멕시코 국민·거주자에게 부여되는 18자리 개인 식별번호. 2025년 개정으로 생체정보 포함 의무 신분증으로 전환.
- 개정안은 CURP를 국가 단일 신원 플랫폼으로 통합하도록 규정했으며, 내무부(Ministry of the Interior)와 디지털전환청(Digital Transformation Agency)이 90일 내 통합 신원 플랫폼(Unified Identity Platform)을 구축하도록 의무화함. 이 플랫폼은 병원·행정기관·학교·이민 절차 등 공공·민간 시스템과 연계돼 본인 확인 인프라로 활용될 예정임. 또한 120일 내 아동·청소년 생체정보 수집 프로그램을 시작해, 실종자 탐색 및 확인 기능 강화를 목표로 함.
- 그러나 인권단체는 이번 조치가 감시사회 확산과 과도한 생체정보 축적으로 이어질 수 있다고 비판함. 특히 개정 법률은 공공기관이 CURP를 조회하거나 접근할 때 당사자에게 통지할 의무를 두지 않아, 데이터 오남용·보안 침해·권한 남용에 대한 통제가 불충분하다는 지적이 제기됨. 디지털권리단체 R3D(Red en Defensa de los Derechos Digitales)와 Article 19는 국가정보센터와 국가경비대 등 치안·정보기관이 생체정보에 직접 접근할 수 있어 사생활 침해 위험이 높아진다고 경고
- 반면 정부는 생체정보는 기존 개인정보보호 체계와 헌법에 따라 보호되며, 위법 활용은 사법적 통제를 받는다고 설명함. 멕시코 대통령은 “통신 감청은 판사 승인 없이는 불가능하다”고 강조하며 제도적 안전장치를 강조
- 개정안은 CURP를 오프라인·디지털 버전으로 모두 발급하도록 규정하고, 모든 공공·민간 기관이 CURP를 신원 인증 수단으로 수용해야 함을 명시함. 이를 통해 금융, 사회보장, 교육, 이민 등 다양한 영역에서 통합적·범용적 신원 인프라를 구축하려는 전략으로 평가됨.
- 이번 개정은 실종자 식별과 공공서비스 효율 개선이라는 목적에도 불구하고, 전 국민 생체정보 중앙집중화에 대한 법적·기술적 보호장치 부재가 핵심 논쟁 지점으로 남을 전망

출처:
· Mexico makes biometric identifier mandatory for all citizens (BiometricUpdate, 2025.07.18.) https://www.biometricupdate.com/202507/mexico-makes-biometric-identifier-mandatory-for-all-citizens#:~:text=Mexico%20has%20officially%20introduced%20a%20digital%20identification%20system,code%20into%20a%20mandatory%20document%20for%20all%20citizens.
· CURP Biométrica: ¿Es Obligatoria? ¿Dónde se Tramita? ¡Aquí las Respuestas a Tus Preguntas! (JUSTIA Mexico, 2025.07.15.) https://mexico.justia.com/blog/curp-biometrica-es-obligatoria-donde-se-tramita-aqui-las-respuestas-a-tus-preguntas/

8월 미국: NIST, 개정된 디지털 신원 지침 발간

❖ 주요 내용



- 2025년 8월 1일, 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)가 개정된 「디지털 신원 가이드라인(Digital Identity Guidelines)」을 공개함. 개정안은 신원 증명·인증·연동 전 단계에 걸친 디지털 신원 보증 수준(Digital Identity Assurance Level)* 달성을 위한 절차적·기술적 요구사항을 전면 재정비한 것이 특징임. 또한 조직 내 신원 관리가 보안·프라이버시·운영 부서가 공동으로 참여하는 교차 기능적(cross-functional) 관리 프로세스임을 명확히 규정하여 신원관리 체계의 구조적 성숙도를 제고하려는 정책적 의도를 나타냄.

  * 디지털 신원 보증 수준(Digital Identity Assurance Level): 온라인 환경에서 개인 신원을 확인·인증하는 과정이 충족해야 하는 신뢰·보안 수준.

- 개정안은 먼저 위험 관리 절차의 재구성을 통해 신원 관련 위험 분석의 맥락 설정을 강화하고 지속 평가 지표를 신규 반영함. 이는 신원 기반 공격 증가, 분산 서비스 환경 확산, 인증자 위협 고도화 등에 대응하기 위한 조치로 평가됨. 신원 증명 단계에서는 사기방지 요건 강화, 역할 기반 증명 절차 명확화, 증빙 자료 검증 체계의 정교화 등을 도입하며, 지식 기반 인증(Knowledge-Based Authentication, KBA)의 한계를 보완하기 위해 비문자적 인증 요소의 활용을 확대
- 또한 개정안은 인젝션 공격·딥페이크 공격 대응 통제를 새롭게 포함함. 이는 생성형 AI 발전으로 인한 신원 위조 가능성 증가를 반영한 것으로, 영상·음성 기반 신원 검증 과정에서의 무결성 검증 절차 및 공격 탐지 기준을 구체화함. 인증 단계에서는 비밀번호 구성·주기 규정이 개편되었으며, 동기화 인증수단(synced authenticators)을 정식 요소로 규정해 기기 간 인증 환경의 일관성과 신뢰성을 강화함.
- 연동(federation) 영역에서는 가입자 제어형 지갑(subscriber-controlled wallet)*** 개념을 도입함. 이는 디지털 자격증명과 인증 정보를 개인이 직접 보관·통제하는 구조로, 신원 연동 모델에서 이용자 통제권 강화라는 글로벌 논의 흐름을 반영한 조치임. 이 지갑은 분산식 신원(Decentralized Identifier, DID) 체계 및 자격증명 생태계와의 상호운용성을 고려해 설계되었으며, 기관 간 신원 전달 과정에서의 투명성과 보안성 향상을 목표로 함.

  ** 가입자 제어형 지갑(subscriber-controlled wallet): 개인이 자격증명 및 인증정보를 직접 보관·관리·제어하는 디지털 지갑 구조
- NIST는 개정 가이드라인이 조직의 신원 위험 관리 수준을 높일 뿐 아니라 개인정보 침해 가능성을 줄이고, 기술 발전에 대응 가능한 신원관리 체계를 수립하는 데 필요한 기준을 제공한다고 설명함. 국내 기관·기업 역시 개정안의 통제 항목과 구조를 참고해 AI·원격 인증·모바일 지갑 기반 환경에서 요구되는 보안·프라이버시 조치를 조기에 구축할 필요성이 제기됨.

출처:
- USA: NIST publishes revised Digital Identity Guidelines (DataGuidance, 2025.08.04.) https://www.DataGuidance.com/news/usa-nist-publishes-revised-digital-identity-guidelines
- Digital Identity Guidelines (NIST, 2025.08.01.) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf

8월 캐나다: OPC, 생체인식 관련 지침 발표

❖ 주요 내용

- 2025년 8월 11일 캐나다 개인정보 감독기관(Office of the Privacy Commissioner of Canada, OPC)이 「생체정보 처리 지침(Guidance on Biometrics)」을 공개함. 본 지침은 연방기관과 기업을 대상으로 생체정보 처리 전 과정의 원칙·절차·책임 기준을 명확히 제시하는 것을 목표로 함.
- 지침은 생체정보를 인간 특성의 정량화 정보(biometrics)로 정의하며, 신체적 특성(physiological biometrics)*과 행동적 특성(behavioral biometrics)**으로 구분함. OPC는 특정 개인을 고유하게 식별하거나 건강·성별 등 민감한 정보를 추론할 수 있는 경우 생체정보를 민감정보로 간주해야 한다고 명시

  * 신체적 생체정보(Physiological Biometrics): 지문·홍채·얼굴·DNA 등 비교적 안정적인 신체적 특징.
  ** 행동적 생체정보(Behavioral Biometrics): 걸음걸이·음성·타자 패턴 등 개인의 행동 기반 특징.
- OPC는 생체정보가 갖는 비가역성, 변조 불가능성, 오·남용 시 고위험성을 고려해 수집·이용 단계에서 특별 보호조치가 필요하다는 점을 강조함. 이를 위해 기업에는 적절한 목적 설정, 이용자 동의 확보, 수집·이용·보관 최소화, 보안조치 강화, 정확성 관리, 책임성과 투명성 확보 등 일련의 준수 의무를 부과
- 지침은 특히 「캐나다 개인정보보호법(Personal Information Protection and Electronic Documents Act, PIPEDA)」의 원칙을 토대로, 최소 수집과 목적 제한 원칙을 재확인함. 기업은 생체정보가 목적 달성에 반드시 필요한지, 덜 침습적인 대안이 존재하는지, 비용·효과·프라이버시 영향이 균형을 이루는지 평가해야 함.
- 생체정보 활용 시에는 자동화된 의사결정 설명, 데이터 이전·보관 절차 공개, 외부 서비스 제공자 관리 등 투명성 확보가 요구됨. 또한 생체정보 시스템은 암호화, 접근통제, 위·변조 방지, 테스트 기반 정확성 검증 등 기술적 안전조치를 포함해야 함.
- 본 지침은 2023년 11월 공청회 과정에서 확보한 시민·기업·법률단체 의견을 반영해 최종 확정된 것으로, OPC는 생체정보 처리의 본질적 고위험성을 고려할 때 목적의 정당성, 수집 최소화, 투명성·동의·책임성 원칙 준수가 필수적이라고 강조함. OPC는 향후 생체정보 기반 서비스 확산에 대비한 지속적 감독과 지침 보완을 예고

출처:
- Canada: OPC publishes guidance on biometrics (DataGuidance, 2025.08.12.) https://www.DataGuidance.com/news/canada-opc-publishes-guidance-biometrics
- Privacy Commissioner of Canada publishes guidance on biometrics (OPC, 2025.08.11.) https://www.priv.gc.ca/en/opc-news/news-and-announcements/2025/nr-c_250811/

11월 미국: EPIC, ICE에 얼굴인식기술 사용 중단 촉구

❖ 주요 내용

- 2025년 11월 26일, 전자프라이버시정보센터(Electronic Privacy Information Center, EPIC)를 포함한 다수 시민단체는 미국 이민관세집행국(U.S. Immigration and Customs Enforcement, ICE)이 현장에서 스마트폰 기반 안면인식 앱 모바일 포티파이(Mobile Fortify)를 사용해 이민 신분을 확인하는 관행이 중대한 개인정보 침해 위험을 초래한다고 지적함. 이 앱은 현장에서 촬영된 얼굴 영상을 즉시 광범위한 통합 데이터베이스와 대조하는 방식으로 작동해 개인이 사실상 비자발적 스캔에 노출되는 구조를 형성하며, 신원 확인 과정 전반에 투명성 결여 문제가 드러난 상황
- 시민단체는 특히 ICE 현장요원이 단일 안면인식 결과만을 이민 신분 판단의 사실상 최종 근거로 삼는 것은 기술적 신뢰도와 법적 절차 보장 측면에서 심각한 위험을 초래한다는 점을 강조함. 안면인식 기술은 인종·성별·조명 조건에 따라 정확도 편차가 크고 오인식률이 높은 특성을 가지는데, 현장 촬영과 같이 비정형 이미지 환경에서는 이 위험이 더욱 심화됨. 이는 구조적으로 유색인종·이민자 집단이 오인식 피해를 집중적으로 겪을 가능성을 높이며, 부당한 구금·추방으로 이어질 위험을 증폭시키는 문제로 지적됨.
- 또한 EPIC 등 단체는 ICE가 모바일 포티파이 도입·운영에 대해 개인정보 영향평가(Privacy Impact Assessment, PIA)를 수행하지 않은 것은 심각한 절차적 위반이라고 비판함. ICE는 기존 시스템에 대한 DPIA 문서로 신규 현장 스캔 프로그램까지 충족된다고 주장했으나, 시민단체는 무작위 현장 촬영, 즉시 대조, 15년간 정보 보관 등은 기존 평가 범위를 명백히 초과하는 요소로, 단순한 개인정보 임계치분석(Privacy Threshold Analysis, PTA)*만으로는 정당화될 수 없다고 지적

  * 개인정보 임계치분석(PTA): 특정 사업·시스템에서 PIA 수행 필요성을 판단하는 사전 검토 절차.
- 아울러 시민단체는 해당 기술이 선택권 제공 없이 일방적으로 신원 수집과 판단에 사용되는 점, 그리고 신원 확인이 사실상 이민 신분 판정과 법적 조치로 직결될 수 있는 점을 지적하며, 이는 표현의 자유 및 집회 참여 권리에 위축 효과를 가져올 수 있다고 경고함. 감시 강화는 이민자·소수자 커뮤니티의 이동·접촉 활동 자체를 억제하는 결과를 초래할 수 있으며, 이는 공권력 행사에 대한 헌법적 우려로 이어질 수 있다는 점이 제기됨.
- 이에 따라 EPIC을 포함한 연대 단체들은 ICE에 대해 모바일 포티파이의 현장 사용 중단, 미국 국토안보부(Department of Homeland Security, DHS)에 대해 관련 정책 문서·평가 자료의 전면 공개를 요구함. 단체들은 이민 집행 과정에서 개인정보 보호와 절차적 권리 보장이 필수적이라는 점을 강조하며, 현장 생체정보 수집 기술 도입 시 법적 근거·평가 절차·감독 체계가 확립되지 않을 경우 심각한 인권 침해가 발생할 수 있다고 경고함.

출처:
- USA: EPIC and others call on ICE to stop use of facial recognition (DataGuidance, 2025.11.27.) https://www.DataGuidance.com/news/usa-epic-and-other-call-ice-stop-use-facial
- Dear Chief Privacy Officer Jankowski (EPIC, 2025.11.25.) https://epic.org/wp-content/uploads/2025/11/Coalition-Letter-on-ICE-Mobile-Fortify-FRT-Nov2025.pdf

4. 연령 확인 및 아동보호

(1) 미국: COPPA 2.0 재상정, 아동·청소년 온라인 개인정보 보호 강화 본격화

(2) 영국: 온라인 유해 콘텐츠로부터 아동 보호를 위한 아동 보호 행동 규약 발표

(3) 호주: 16세 미만 아동의 SNS 금지 시행

(4) 스페인: 아동 온라인 보호 및 연령 확인 관련 포괄적 법률 도입

(5) 미국: 인공지능 및 아동 개인정보 보호 위한 안전조치 기준 발표

3월 미국: COPPA 2.0 재상정, 아동·청소년 온라인 개인정보 보호 강화 본격화

❖ 주요 내용

- 2025년 3월 4일, 미국 상원의원 에드 마키(Ed Markey)와 빌 캐시디(Bill Cassidy)는 「아동·청소년 온라인 프라이버시 보호법(Children and Teens' Online Privacy Protection Act, COPPA 2.0)」을 미 상원에 재상정함. 이 법안은 1998년 제정된 「아동 온라인 프라이버시 보호법(Children's Online Privacy Protection Act, COPPA)」을 개정해 보호 대상을 기존 만 13세 미만 아동에서 만 16세 미만 청소년까지 확대하고, 플랫폼의 책임 기준과 집행 체계를 전면적으로 강화하는 것을 목표로 함.
- 법안은 아동·청소년을 대상으로 한 개별 맞춤형 타깃 광고를 전면 금지하고, 사업자가 수집한 아동·청소년의 개인정보를 이용자 또는 보호자의 요청에 따라 손쉽게 삭제하도록 '지우개 버튼(Eraser Button)'* 기능을 의무화함. 또한 개인정보 수집·이용을 서비스 제공에 필수적인 범위로 제한하는 데이터 최소화(Data Minimization)** 원칙을 명문화하고, 서비스 품질 향상·행태 분석 등 부수적 목적을 위한 광범위한 정보 수집 관행을 제약

  * 지우개 버튼(Eraser Button): 아동·청소년 또는 보호자가 플랫폼에 저장된 개인정보 삭제를 간편하게 요청·실행할 수 있도록 한 온라인 삭제 기능

  ** 데이터 최소화(Data Minimization): 서비스 제공에 필수적인 범위를 넘는 개인정보 수집·이용을 금지하고, 목적 달성에 필요한 최소한의 정보만 처리하도록 요구하는 원칙.
- 플랫폼의 연령 인지 의무도 강화됨. 기존 COPPA가 사업자의 '실제 지식(Actual Knowledge)'이 있는 경우에만 규제를 적용했다면, COPPA 2.0은 이용자가 아동·청소년임을 합리적으로 인지할 수 있는 상황, 즉 '구성적 지식(Constructive Knowledge)'이 있는 경우까지 책임 범위를 확장함. 이에 따라 청소년 이용자가 다수인 플랫폼이 고의로 연령 정보를 수집하지 않으면서 규제를 회피하던 관행을 차단하려는 취지로 해석됨.
- 집행 체계 측면에서 법안은 미국 연방거래위원회(Federal Trade Commission, FTC)에 전담 조직을 두어 아동·청소년 대상 마케팅 및 개인정보 처리 행위를 집중 감독하도록 하고, 위반 사업자에 대한 제재 수준과 보고 의무를 상향 조정함. 동시에 학교·교육기관이 적법한 교육 목적 범위에서 서비스 이용을 위탁할 수 있도록 예외 규정을 정비해, 온라인 학습 환경에서의 합리적인 정보 활용과 보호의 균형을 도모하려는 방향을 제시함.
- 입법 진행 상황을 보면, 2025년 6월 COPPA 2.0은 상원 상무·과학·교통위원회에서 수정안을 포함해 찬성 의결을 받고 본회의 상정을 대기 중인 상태임. 하원에서도 유사한 내용의 법안이 발의되어 2025년 12월 청문회가 진행되는 등 논의가 이어지고 있으나, 광범위한 연방·주 법률과의 정합성, 부모 동의 권한 범위, 민사소송 허용 여부 등을 둘러싼 이해관계가 복잡해 연내 최종 타결 여부는 불투명한 상황으로 평가됨. 그럼에도 양당 의원 다수와 의료·교육·시민단체의 지지가 견고해 중장기적으로는 아동·청소년 온라인 개인정보 보호 기준을 실질적으로 상향 조정하는 핵심 법안으로 작용할 가능성이 큼.

출처:
- USA: COPPA 2.0 reintroduced in Senate (DataGuidance, 2025.03.06.) https://www.DataGuidance.com/news/usa-coppa-20-reintroduced-senate
- How Congress Can Protect Children from Predatory Social Media and Pornography Platforms (heritage, 2025.11.26.) https://www.heritage.org/big-tech/report/how-congress-can-protect-children-predatory-social-media-and-pornography-platforms

4월 영국: 온라인 유해 콘텐츠로부터 아동 보호를 위한 아동 보호 행동 규약 발표

❖ 주요 내용

- 2025년 4월 24일, 영국 통신규제기관 오프콤(Office of Communications, Ofcom)은 「온라인 안전법(Online Safety Act 2023)」에 따른 「아동 보호 행동 규약(Protection of Children Codes)」을 발표하고, 2025년 7월 25일부터 법적 효력을 갖는 아동 온라인 보호 기준을 시행함. 이번 규약은 영국 내 아동(만 18세 미만)이 이용할 가능성이 있는 이용자 간 서비스(user-to-user services)*와 검색 서비스 전반에 대해 아동 유해 콘텐츠 노출 위험을 체계적으로 평가·완화하도록 의무를 부과하는 포괄적 규율 체계로 기능

  * 이용자 간 서비스(user-to-user services): 이용자가 게시한 콘텐츠를 다른 이용자가 접할 수 있도록 하는 서비스로, 소셜미디어, 동영상 공유 플랫폼, 온라인 커뮤니티 등 상호작용형 플랫폼 전반을 포괄하는 개념

- 규약은 소셜미디어, 동영상 공유 플랫폼, 온라인 게임, 검색엔진 등 아동 접근 가능 서비스 제공자에게 아동 위험 평가 의무를 부과하고, 2025년 7월 24일까지 서비스별 아동 위험 평가를 완료·기록하도록 요구함. 이후 7월 25일부터는 규약에 명시된 안전 조치를 이행하거나, 동등한 보호 효과를 입증할 수 있는 대체 조치를 적용해야 하며, 이는 단순 권고가 아닌 「온라인 안전법(Online Safety Act 2023)」상 법적 의무로 작동

- 콘텐츠 측면에서 규약은 유해 콘텐츠를 '포르노·자살·자해·섭식장애 등 1차 우선 유해 콘텐츠', 괴롭힘·증오·폭력 조장 등 '우선 유해 콘텐츠', 우울·절망 조장 등 기타 '비지정 유해 콘텐츠'로 구분하고, 아동 연령대별 노출 위험을 평가해 피드·추천·검색 결과에서 해당 콘텐츠를 차단·필터링할 것을 요구함. 특히 추천 알고리즘을 운영하는 경우, 중·고위험 서비스는 아동 피드에서 유해 콘텐츠를 효과적으로 걸러낼 수 있는 콘텐츠 필터링·우선순위 조정 체계를 갖출 것을 요구

- 연령 확인·검증 측면에서는 고위험 서비스에 대해 고도화된 연령 확신·검증 기술(age assurance technologies)을 도입해 아동 이용자를 식별하고, 연령대에 따른 차등 보호 조치를 제공할 것을 요구함. 강력한 연령 확인이 없는 서비스는 아동 이용자가 존재하는 것으로 전제하고 설계를 해야 하며, 아동에게는 계정 차단·음소거, 원치 않는 그룹 초대 거부, 댓글 비활성화, 유해 콘텐츠 표시 최소화 등 자율 통제 기능을 기본 제공하도록 규정

- 거버넌스 측면에서 각 사업자는 아동 보호를 담당하는 책임자를 지정하고, 이사회·경영진 수준에서 정기적으로 아동 위험 관리 체계를 검토할 의무를 부담함. 위험 평가 결과와 이행 조치는 문서화·보관해야 하며, 이용자가 유해 콘텐츠를 손쉽게 신고하고 사업자가 신속히 평가·조치할 수 있는 신고·불만 처리 절차를 마련해야 함. 규약을 위반하는 경우 최대 1,800만 파운드 또는 전 세계 매출액의 10% 중 높은 금액까지 과징금 부과가 가능하며, 심각한 위반 시 서비스 차단 등 추가 제재도 허용됨.

출처:
- UK: Ofcom publishes child safety Codes of Practice under Online Safety Act (DataGuidance, 2025.4.24.) https://www.DataGuidance.com/news/uk-ofcom-publishes-child-safety-codes-practice-under
- New rules for a safer generation of children online (Ofcom, 2025.4.24.) https://www.ofcom.org.uk/online-safety/protecting-children/new-rules-for-a-safer-generation-of-children-online?utm_source=linkedin&utm_medium=social-media&utm_campaign=onlinesafety24&utm_content=protectingchildren

6월 호주: 16세 미만 아동의 SNS 금지 시행

❖ 주요 내용

- 호주는 2025년 12월 10일 시행 예정인 16세 미만 소셜미디어 전면 금지 정책 이행을 위해 연령확인 기술 실증시험을 완료한 상태임. 해당 정책은 플랫폼에 '연령 차단을 위한 합리적 조치' 이행 의무를 부과하며, 미준수 시 최대 4,950만 호주달러 또는 글로벌 매출 10% 과징금 부과 가능성 존재
- 실증시험은 영국 인증기관 에이지 체크 서티피케이션 스킴(Age Check Certification Scheme, ACCS)이 주관한 시험으로, 1,000명 이상 청소년을 대상으로 약 60종 연령확인 소프트웨어의 정확성·우회 가능성·적합성 검증을 포함함. 그 결과, 신용카드 확인이나 생년월일 입력보다 얼굴 기반 연령추정 기술이 가장 높은 정확도(최대 99%대)를 기록한 것으로 확인됨. 다만 특정 제품에서 10대가 성인으로 판정되는 사례가 존재해 기술 신뢰 기준 마련 필요성이 제기됨.

- 청소년 참여자들은 기술적 정확성과 별개로, 형제자매 사진 제출, 기기 우회, VPN 활용 등 차단 회피 가능성이 상존함을 지적함. 이는 연령확인 기술이 완전 차단보다 위험 완화 기능에 더 적합하다는 평가로 이어짐.
- 법적 논쟁도 진행 중임. 자유주의 성향 단체 디지털 프리덤 프로젝트(Digital Freedom Project)는 15세 청소년을 대리해 소송을 제기하며, 연령제한 정책이 청소년의 정치적 표현의 자유 침해에 해당한다는 주장을 전개함. 해당 단체는 정부 정책이 "국가가 부모 역할을 대체하는 조치"라는 비판을 표명함. 반면 정부는 아동·청소년 정신건강 보호 필요성을 우선 가치로 제시
- 여론은 규제 강화에 상당한 지지 기반을 형성함. 부모의 68%가 16세 미만 소셜미디어 금지 찬성 입장을 표명한 조사 결과가 존재함. 유럽 및 아시아 주요국과 미국 일부 주도 유사 정책을 검토 중으로, 호주의 정책이 국제 연령확인 규제 논의에 선례적 영향력을 행사할 가능성 존재
- 한편 호주 개인정보 감독기관(Office of the Australian Information Commissioner, OAIC)은 「아동 온라인 프라이버시 코드(Children's Online Privacy Code)」 제정을 위해 아동·청소년·부모·산업계 대상 단계별 의견수렴 절차를 진행 중임. 해당 코드는 플랫폼에 대한 연령 적합 설계 의무, 프라이버시 기본 보호설정 의무, 투명성 강화 요구 등을 포함하는 규범으로 기능 예정

출처:
· Australia's teen social media ban faces a new wildcard: teenagers (Reuters, 2025.06.24.)
https://www.reuters.com/world/asia-pacific/australias-teen-social-media-ban-faces-new-wildcard-teenagers-2025-06-19/
· Australian opposition politician challenges age checks for social media (Biometricupdate, 2025.11.27.)
https://www.biometricupdate.com/202511/australian-opposition-politician-challenges-age-checks-for-social-media
· Children and parents told the OAIC that online privacy matters (OAIC, 2025.11.20.)
https://www.oaic.gov.au/news/media-centre/children-and-parents-told-the-oaic-that-online-privacy-matters

7월 스페인: 아동 온라인 보호 및 연령 확인 관련 포괄적 법률 도입

❖ 주요 내용

- 스페인 정부는 2024년 7월 아동·청소년의 온라인 안전 강화를 목표로 한 「디지털 환경에서의 미성년자 보호 기본법(Organic Law for the Protection of Minors in Digital Environments)」 초안을 최초 공개함. 이후 의견 수렴과 기술 검토를 거쳐, 2025년 3월 25일 각료회의가 개정안을 승인함에 따라 법안은 의회 심사 단계(parliamentary phase)로 공식 이송된 상태임. 현재 최종 입법 절차가 진행 중이며, 향후 표결을 통해 시행 여부가 확정될 예정
- 법안은 만 16세 미만 미성년자의 소셜미디어 이용 원칙적 제한, 연령대별 콘텐츠 접근 통제, 기기 초기 설정 단계에서 활성화되는 부모통제 기능 등 다층적인 보호체계를 구성함. 기기 제조사에는 무료이면서 효과적인 부모통제 기능을 기본값(default)으로 탑재할 의무가 부과되며, 설정 과정에서 수집되는 데이터의 상업적 활용 금지가 명문화됨.
- 온라인 플랫폼과 디바이스 제조사는 연령확인 시스템 도입 전 개인정보 영향평가(Data Protection Impact Assessment, DPIA)를 수행해야 하며, 연령확인은 단말기 내 비식별 방식으로 처리되어야 함. 성별·인종 등 추가 정보 요구, 중앙 집중형 데이터 저장, 프로파일링, 지속적 추적 등은 금지됨.
- 인터랙티브 플랫폼, 게임 등에서는 랜덤 보상 메커니즘(Random Reward Mechanisms)* 및 루트박스(loot box)** 활성화에 대해 18세 미만 제한 규제가 적용됨. 인플루언서 및 팔로워 규모가 큰 콘텐츠 제작자는 스폰서 표시 의무, 유해 콘텐츠 게시 제한, 아동 이용자 보호 조치 마련 등 추가 규제가 부과됨.

  * 랜덤 보상 메커니즘(Random Reward Mechanisms): 게임 내에서 무작위 확률에 기반해 보상을 제공하는 모든 시스템을 포괄하는 개념으로, 확률형 아이템·랜덤 뽑기 등 다양한 형태를 포함

  ** 루트박스(loot box): 랜덤 보상 메커니즘의 대표적 유형 중 하나로, 상자를 열었을 때 무작위 보상이 제공되는 방식. 도박 유사성·중독성 우려로 미성년자 대상 규제에서 중점 관리 대상으로 분류됨.
- 법안은 아동 대상 온라인 성적 착취물·AI 딥페이크 생성 및 유포 금지, 사이버 스토킹 처벌 강화, 학교 내 스마트기기 사용 규율, 디지털 리터러시 교육 확대 등 종합적인 보호 조치를 포함함. 아울러 성별 기반 폭력 피해 아동 지원 체계 강화와 24시간 상담 서비스 제공 의무도 포함됨.
- 감독체계는 스페인 개인정보 감독기관(Agencia Española de Protección de Datos, AEPD)이 개인정보 보호 준수를 총괄하고, 국가시장경쟁위원회(National Commission on Markets and ComPETsition, CNMC)가 연령확인 시스템의 기술적 적정성 평가를 담당하는 구조로 설계됨.

출처:
- Spanish law among most comprehensive for age checks, kids' online safety (BiometricUpdate, 2025.06.23.) https://www.biometricupdate.com/202506/spanish-law-among-most-comprehensive-for-age-checks-kids-online-safety
- Understanding age assurance in Spain's new online safety law (YOTI, 2025.06.18.) https://www.yoti.com/blog/age-assurance-spain-online-safety-organic-law/

10월 미국: 인공지능 및 아동 개인정보 보호 위한 안전조치 기준 발표

❖ 주요 내용

- 미국 아동광고심의위원회(Children's Advertising Review Unit, CARU)*는 2025년 10월 20일 '생성형 인공지능 & 아동 위험 매트릭스(Generative AI & Kids Risk Matrix)'를 발표함. CARU는 전미광고자율심의기구(BBB National Programs)* 산하 조직으로, 아동 대상 광고와 데이터 보호 기준을 정립하는 규제·자율심의 기관임.

  * 전미광고자율심의기구(BBB National Programs): 미국 민간 자율규제 기구로 광고, 소비자 보호, 아동 온라인 안전 관련 기준을 마련하는 조직.

- 이번 매트릭스는 장난감·게임·스트리밍·모바일·광고기술(adtech) 등 글로벌 기업이 참여한 AI 워킹그룹(AI Working Group)이 15개월간 개발한 안전조치 체계로, 생성형 인공지능 이용 과정에서 아동에게 발생할 수 있는 개인정보 침해, 부적절 콘텐츠 노출, 편향 및 조작 위험 등을 체계적으로 분류하고 단계별 대응방안을 제시

- 식별된 핵심 위험 분야는 ▲허위·기만적 광고 ▲인플루언서 조작 ▲프라이버시 침해 ▲AI 편향 및 차별 ▲정신건강 훼손 ▲과도한 상업화 ▲유해 콘텐츠 노출 ▲투명성 결여 등임. 매트릭스는 각 위험에 대해 구체적 피해 사례, 잠재적 결과, 기업 책임, 위험 완화 조치를 제시하여, 기업이 CARU의 광고·프라이버시 가이드라인을 실무적으로 적용할 수 있도록 설계됨.

- CARU는 본 매트릭스가 아동 대상 AI 서비스 개발·운영 시 준수해야 할 윤리·보호 기준의 사실상 업계 표준이 될 것이라고 평가함. 부모·보호자가 아동의 생성형 AI 이용 과정에서 발생 가능한 위험을 이해하고 적절히 대응할 수 있도록 돕는 기능도 강조됨.

- 또한 CARU는 향후 AI 워킹그룹을 산업자율규제센터(Center for Industry Self-Regulation, CISR) 산하로 확대할 계획임. 이에 따라 연구자·학계 전문가가 추가 참여하여 AI 챗봇·AI 동반자(AI companions) 등 청소년 이용률이 높은 서비스의 위험 평가 및 윤리적 활용 기준이 강화될 전망임. CISR 체계 하에서 CARU는 아동·청소년 대상 AI 서비스 전반에 대한 지속적 모니터링 및 업계 자율규범 고도화를 추진할 예정

- 종합적으로 이번 매트릭스는 기업의 아동 대상 광고·데이터 처리 관행을 투명성·안전성 중심으로 재편하는 전환점이 될 것으로 평가되며, 생성형 AI 확산 속에서 아동권리 보호의 최소 기준을 제시하는 자율규제 기준으로 기능할 것으로 예상됨.

출처:
- USA: CARU releases safeguards for AI and children's data (DataGuidance, 2025.10.24.) https://www.DataGuidance.com/news/usa-caru-releases-safeguards-ai-and-childrens-data
- BBB National Programs' Children's Advertising Review Unit Publishes Safeguards for Generative AI & Kids; Announces Expanded AI Working Group (CARU, 2025.10.20.) https://bbbprograms.org/media/newsroom/press/generative-ai-kids

5. 데이터 활용 기술

(1) 교통카드 공공 합성데이터 첫 개방

(2) 유럽 넘어 한국까지 확산되는 '소버린 클라우드'

(3) 공공 AI의 주축으로 떠오른 ‘소버린 AI’, 해외 주요 국가 동향은

(4) 디지털 보호주의 '급부상'…데이터 장벽 더 높아진다

3월 교통카드 공공 합성데이터 첫 개방

❖ 주요 내용

- 2025년 공공데이터 정책은 '국가중점데이터* 개방'을 중심으로 교통·산업·공정거래 전반에서 데이터 활용 기반을 확장하는 방향으로 전개됨.

  * 국가중점데이터: 사회·경제적 효과가 큰 고가치 공공데이터를 정부가 선별해 개방 대상으로 지정한 데이터.

- 3월 19일, 국토교통부·교통안전공단·한국지능정보사회진흥원은 국내 최초로 교통카드 합성데이터(Synthetic Data)**를 포함한 65개 항목을 개방하며 정책의 출발점을 열었음. 제공 범위는 ▲교통카드 이용량 ▲통행시간·거리 ▲노선 및 정류장 정보 ▲출발지-도착지 수요 ▲응용데이터이며, 원본 공개 대신 합성데이터 방식으로 개인정보 침해 위험을 차단하는 구성이 특징임. 수도권에서 우선 제공을 시작해 전국으로 확대할 계획이며, 상권 분석, 배차 최적화, 교통약자 이동 패턴 분석 등 다양한 공공·민간 서비스 개선으로 이어질 전망

  ** 합성데이터(Synthetic Data): 원본 데이터의 통계적 특성을 모방해 개인정보 없이 인공적으로 생성한 데이터.

- 이어 7월 행정안전부는 AI 학습과 기업 지원을 위한 고가치 데이터 15종을 국가중점데이터로 선정함. 개방 대상은 ▲중앙부처 법령해석 및 특별행정심판 재결례 ▲특수교 계측 데이터 ▲발전소 운영 정보 등 AI 학습용 데이터와 ▲전국 인허가 정보 ▲생활편의 정보 ▲항만 운항정보 ▲농산물 유통정보 ▲건물 화재예방·대응시설 정보 등 기업 활용도가 높은 데이터로 구성됨. 개인정보 포함 데이터는 합성데이터 또는 진위확인 방식을 활용하여 안전하게 개방하는 방향으로 추진됨. 정부는 AI 서비스 개발 수요가 높은 분야를 중심으로 'AI·고가치 공공데이터 Top 100'을 설정해 단계적 개방을 지속할 예정

- 12월 공정거래위원회는 공정거래 데이터포털(FairData)*** 정비 계획을 발표하며 공공데이터 개방과 생성형 AI 도입을 본격 추진함. 개방 확대 범위는 ▲통계연보 ▲정형통계 ▲의결서 관련 데이터 등 사건 중심 정보로, 국민과 기업의 검색 접근성을 높이기 위한 조치임. 내부적으로는 빅데이터 분석 플랫폼을 고도화하고 분석전문가를 배치해 사건처리 지원체계를 강화할 계획임. 또한 생성형 AI 기반 기능을 도입해 ▲자연어 질의응답 ▲민원 추천 ▲사건보고서 작성지원 ▲약관심사 보조 ▲AI 번역 ▲유사 심결례·판례 검색을 제공할 예정이며, 데이터 품질 보정과 메타데이터 기반 학습을 거쳐 2026년 하반기 실제 서비스로 이어질 계획

  *** 공정거래 데이터포털(FairData): 공정거래위원회가 의결서·통계 등 경쟁정책 데이터를 개방하기 위해 운영하는 공식 포털.

- 공공데이터 전반에서 합성데이터 도입, 기계판독 기반 개방 강화, AI 활용 고도화를 동시에 추진하는 구조적 변화로 이어지는 양상임. 데이터 안전성을 확보하면서도 활용성을 극대화하는 방향으로 정책이 정렬되고 있으며, 교통·산업·규제 행정까지 전 영역에서 데이터 기반 의사결정 체계가 강화되는 결과로 연결되는 흐름임.

출처:
- 교통카드 공공 합성데이터 첫 개방 교통대책 등 활용 (뉴시스, 2025.03.19.) https://n.news.naver.com/mnews/article/003/0013127630?sid=101
- 정부, AI 학습·기업 지원용 고가치 공공데이터 15종 개방키로 (연합뉴스, 2025.07.29.) https://n.news.naver.com/mnews/article/001/0015535970?sid=101
- 공정위, 데이터포털 정비…내년 하반기 생성형 AI 본격 도입 (이데일리, 2025.12.09.) https://n.news.naver.com/mnews/article/018/0006179881?sid=101

4월 유럽 넘어 한국까지 확산되는 '소버린 클라우드'

❖ 주요 내용

- 유럽을 중심으로 데이터 주권 확보 요구가 강화되며 소버린 클라우드(Sovereign Cloud)* 도입이 확대되는 상황임. 소버린 클라우드는 데이터를 자국 내에서만 저장·관리해 외부 접근을 차단하는 구조로, 규제 준수와 통제권 강화를 목표로 하는 인프라 모델임. 유럽연합(EU)은 아마존웹서비스(Amazon Web Services, AWS), 마이크로소프트 애저(Microsoft Azure), 구글 클라우드(Google Cloud) 의존에서 벗어나기 위한 자체 생태계 구축을 추진 중이며 데이터 경쟁력 확보를 국가 전략으로 간주하는 흐름이 나타나는 중임.

  * 소버린 클라우드(Sovereign Cloud): 데이터를 자국 내에서만 저장·관리해 외국의 접근을 차단하는 국가 데이터 주권형 클라우드 인프라.

- EU 공공·행정기관에서는 외국 정부의 데이터 요구 가능성, 관세 부과에 따른 인프라 비용 증가, 서비스 제한권 등 위험 요인을 문제로 제기하는 상황임. 생성형 인공지능 확산과 함께 데이터 통제력이 국가 경쟁력과 직결된다는 인식이 커지며 소버린 클라우드 필요성이 지속적으로 상승하는 추세임. 미국 기업 중심의 하이퍼스케일러 구조에서 벗어나기 위한 규제 정비와 자국 클라우드 전환 움직임이 병행되는 상황
- 국내에서도 소버린 클라우드 확산 경향이 명확히 드러남. 국내 클라우드 서비스 제공자(CSP)는 공공기관의 클라우드 보안 인증(Cloud Security Assurance Program, CSAP)을 기반으로 이미 소버린 요건을 충족하는 인프라를 제공해 왔으며, 공공뿐 아니라 민간에서도 프라이빗과 퍼블릭을 결합한 모델 수요가 증가하는 추세임. 유럽이 해외 CSP 의존에서 벗어나기 위한 전환을 추진하는 상황과 대비해 국내에서는 조기 정착이 이루어진 구조
- 국내 기업 중 네이버클라우드(Naver Cloud)는 뉴로클라우드(Neuro Cloud) 기반 소버린 전략을 강화하고 있으며 하이퍼클로바X(HyperCLOVA X) 구축형 모델을 공공·금융 영역에 공급 중임. 또한 소버린 AI 전략을 기반으로 국내뿐 아니라 해외 지역에서도 맞춤형 AI 환경 조성을 확대하는 방향으로 사업을 확장하는 중임. LG유플러스(LG Uplus)는 AWS와 협력해 한국형 소버린 클라우드 개발에 참여하며 공공·금융 중심 AI 전환 요구에 대응하는 중임.
- 2025년 11월 12일, KT는 마이크로소프트와의 협력으로 시큐어 퍼블릭 클라우드(Secure Public Cloud)를 개발해 국내에 출시함. 시큐어 퍼블릭 클라우드는 기밀 컴퓨팅 적용, 관리형 하드웨어 시큐리티 모듈 기반 전용 키 관리, 국내 저장 원칙 등 소버린 요구사항을 반영한 서비스로 구성됨.
- 기업은 고도화된 AI 시스템 통합 과정에서 데이터 보호와 내부 통제 요구를 충족해야 하는 상황임. 데이터 중력(Data Gravity)**, 모델 훈련 경계 설정, 맞춤형 AI 개발 환경 구축 등 다양한 요구를 충족하는 기반으로 소버린 클라우드 필요성이 강화되는 추세임. 소버린 클라우드가 AI 활용 구조의 중심 축으로 자리 잡으며 기술 진화와 규제 요구를 동시에 대응하는 핵심 인프라로 부상하는 양상

  ** 데이터 중력(Data Gravity): 데이터가 특정 환경에 축적될수록 시스템·서비스가 그 환경으로 끌려가는 현상.

출처:
- "데이터 주권 지킨다"…유럽 넘어 한국까지 확산되는 '소버린 클라우드' (지디넷코리아, 2025.04.22.) https://n.news.naver.com/mnews/article/092/0002371666?sid=105
- KT, '시큐어 퍼블릭 클라우드' 국내 출시 (디지털타임스, 2025.11.12.) https://n.news.naver.com/mnews/article/029/0002993045?sid=105
- AI 시대, '소버린 클라우드'가 기업 생존 좌우한다 (토큰포스트, 2025.12.04.) https://www.tokenpost.kr/news/ai/311117

6월 공공 AI의 주축으로 떠오른 '소버린 AI', 해외 주요 국가 동향은

❖ 주요 내용

- 소버린 AI(Sovereign AI)는 국가가 외국 기술에 종속되지 않고 자국 내에서 통제·운영할 수 있도록 구축하는 독립형 AI 체계를 의미하며, 글로벌 경쟁 심화 속에서 핵심 전략으로 부상함. 특히 개인정보 기반 학습체계의 신뢰 확보가 주요 과제로 제기되며, 데이터센터·GPU(Graphics Processing Unit) 인프라·전문 인력·개인정보 활용 제도 등이 필수 조건으로 지목됨. 이러한 요구는 데이터 식민주의(Data Colonialism)* 우려가 확대되는 환경에서 국가 단위 자율성 확보 필요성과 맞물려 부각되는 중

  * 데이터 식민주의(Data Colonialism): 특정 국가·기업이 타국·사회의 데이터를 독점해 권력·통제력을 행사하는 구조.

- EU는 GDPR과 EU AI법(EU AI Act)을 기반으로 공동 데이터 활용과 국가별 분산 개발을 병행하며 주권성과 다양성 확보를 추진함. 2025년 2월에는 2,000억 유로 규모의 '인베스트 AI 이니셔티브'를 발표해 AI 기가팩토리(AI Gigafactory)** 설립과 GenAI4EU 프로그램***을 가동하고 있으며, 프랑스와 독일은 엔비디아와의 GPU 대규모 도입 계약을 체결해 인프라 우위를 확보하는 데 집중하고 있음. 영국은 2025년 1월 'AI 기회 실행 계획'을 수립하고 소버린 AI 전담 부서 신설, 슈퍼컴퓨터 구축, AI 보안 연구소 투자 등을 국가 전략으로 채택

  ** AI 기가팩토리(AI Gigafactory): 대규모 AI 학습·추론 인프라를 집적한 초대형 AI 생산 시설.

  *** GenAI4EU: EU 14개 산업·공공 부문에서 공동으로 활용할 생성형 AI 기술과 응용서비스를 개발하는 EU 주도 범유럽 공동 AI 프로젝트.

- 아시아에서도 소버린 AI 정책이 국가 주도 방식으로 확산되는 중임. 일본은 2024~2025년 소프트뱅크에 대한 정부 투자를 통해 일본어 기반 소버린 모델을 개발하고, 'AI 연구·개발 및 활용 촉진법안'을 통해 개인정보 유출 및 허위정보 확산 대응 체계를 규정함. 인도는 2024년 '인디아AI'를 출범시키고 16조 원 규모 예산으로 공공 AI 인프라·LLM 개발·AI 전문교육 체계를 통합 추진하며, 동남아시아는 싱가포르 주도로 '씨라이언 AI'라는 지역 연합형 LLM 개발을 진행 중임. 중동 지역에서는 UAE의 AI71, 사우디아라비아의 대규모 인프라 투자 등 독자 모델 개발 경쟁이 가속화되는 양상

- 국내에서는 소버린 AI 추진 필요성이 중앙정부와 산업계 전반에서 강조되는 분위기임. 2025년 6월 울산 AI 데이터센터 출범식에서 정부는 대규모 AI 인프라 확충과 한국형 LLM 개발을 국가 전략으로 제시하며, 외산 AI 의존이 가져올 국가 차원의 리스크를 경고함. 2025년 11월 열린 경제 포럼에서도 국내 전문가들은 중견국 생존을 위한 필수 전략으로 소버린 AI를 지목하며, 자체 데이터·인프라·개발 생태계 구축의 시급성을 강조

- 이러한 흐름 속에서 소버린 AI는 특정 모델 개발에 국한되지 않고 ▲자국 데이터의 통제권 확보 ▲신뢰 기반 인공지능 환경 조성 ▲맞춤형 AI 모델 구축을 위한 안전한 개발 경계선 제공 등 국가 역량 전반을 좌우하는 구조적 전략으로 자리 잡는 중임. 글로벌 AI 경쟁이 무기화 단계로 진입하는 상황에서 소버린 AI는 기술 자립과 데이터 주권을 동시에 확보하기 위한 핵심적 방어 수단으로 평가됨.

출처:
- 공공 AI의 주축으로 떠오른 '소버린 AI', 해외 주요 국가 동향은 (동아일보, 2025.06.23.) https://n.news.naver.com/mnews/article/020/0003643188?sid=105
- "AI 경쟁 시대에 韓 생존하려면 소버린 AI 전략 필수" (아시아경제, 2025.11.28.) https://n.news.naver.com/mnews/article/277/0005686108?sid=101

8월 디지털 보호주의 '급부상'…데이터 장벽 더 높아진다

❖ 주요 내용

- AI 시대 본격화로 데이터가 국가 경쟁력의 핵심 자원으로 부상하면서 주요국은 데이터 주권(Data Sovereignty) 강화를 전략적 과제로 채택하는 흐름을 보임. 데이터가 국경을 넘어 이동하는 기존 구조가 안보·기술 패권과 직접 연결되면서 각국은 법제 정비를 통해 통제력을 강화하는 추세가 확산됨.

  * 데이터 주권(data sovereignty): 데이터가 발생한 국가가 데이터의 저장·이전·활용을 통제할 권리.

- 미국은 국가 안보를 근거로 데이터 해외 이전을 제한하며, 특히 「클라우드법(Clarifying Lawful Overseas Use of Data Act, CLOUD Act)」을 통해 미국 기업이 보관하는 데이터에 대한 역외 수사권을 확보함. 그러나 연방 차원의 개인정보보호법 부재로 주별 규제가 상이해 기업 불확실성이 지속되는 상황.
- EU는 GDPR을 통해 개인정보 보호 체계를 확립했고, 2025년 시행되는 「데이터법(Data Act)」으로 산업 데이터 활용까지 규율 범위를 확대함. 이에 따라 글로벌 기업은 현지 규제 충족을 위해 소버린 리전 구축 등 분산 운영 전략을 채택하는 양상.
- 중국은 「데이터보안법(Data Security Law)」과 「개인정보보호법(Personal Information Protection Law, PIPL)」을 통해 핵심 데이터의 국내 보관을 원칙으로 하고, 개인정보 10만 명 이상 또는 민감정보 1만 명 이상 포함 시 국가안보 심사를 의무화함. 사실상 전략 데이터의 해외 반출을 차단하는 구조.
- 인도는 디지털 개인정보보호법(Digital Personal Data Protection Act, DPDP Act)을 제정해 허용 국가 목록(Whitelist) 방식의 이전 규제를 도입함. 일본 역시 개인정보보호법(Act on the Protection of Personal Information, APPI)을 개정해 해외 이전 시 상대국 보호 수준 고지·점검을 의무화
- 해외 규제 강화와 더불어 기업 간 데이터 확보 경쟁도 가속되는 흐름. 생성형 AI 경쟁 심화로 고품질 데이터가 부족해지면서 언론사·플랫폼 간 계약 체결과 저작권 분쟁이 증가하는 추세. 국가 단위에서도 데이터 통제 강화가 두드러지며 글로벌 AI 생태계의 단일 운영은 점차 어려워지는 방향.
- 국내에서도 데이터 주권 논쟁이 본격화되는 상황. 2025년 구글과 애플이 고정밀 지도 데이터의 해외 이전을 재요청하면서 안보와 산업 경쟁력 간 균형이 사회적 논제로 부상함. 정부는 데이터 주권을 소버린 AI(Sovereign AI) 전략의 핵심 기반으로 규정하고 GPU·데이터·인재 중심의 생태계 구축을 추진 중

출처:
- [데이터 주권] 디지털 보호주의 '급부상'…데이터 장벽 더 높아진다 (지디넷코리아, 2025.08.20.) https://n.news.naver.com/mnews/article/092/0002386884?sid=105
- [데이터 주권] 왜 '데이터'가 AI 시대의 핵심 자원인가 (지디넷코리아, 2025.08.19.) https://n.news.naver.com/mnews/article/092/0002386733?sid=105
- [기고] 인공지능과 데이터 주권 (지디넷코리아, 2025.11.22.) https://n.news.naver.com/mnews/article/092/0002399468?sid=105

KISA 한국인터넷진흥원

2025년도 개인정보 기술동향

「2025년도 개인정보 기술동향 보고서」는
개인정보보호위원회의 출연금으로 수행한 사업의 결과물입니다.

발행일 2025년 12월
발행처 한국인터넷진흥원
발행처 전라남도 나주시 진흥길 9