

PRiVACY REPORT

개인정보보호 월간동향분석

2024년 5월호



| CONTENTS |

2024년 5월호

1

미국 연방 개인정보 보호법(APRA) 주요 내용 분석

2

EDPS 2023 연례보고서 분석

미국 연방 개인정보 보호법(APRA) 주요 내용 분석



[목 차]

1. 도입 배경 및 개요

2. APRA 주요 내용

- (1) 적용 범위
- (2) 개인정보 최소화 원칙
- (3) 인공지능 관련 의무사항
- (4) 데이터 브로커 관련 의무사항
- (5) 애드테크 관련 의무사항
- (6) 사적 소송권
- (7) 집행 및 감독
- (8) 개인정보보호 강화 감사 파일럿 프로그램

3. 결론 및 시사점

1. 도입 배경 및 개요

■ 미국 하원의 캐시 맥모리스 로저스(Cathy McMorris Rodgers) 에너지상업위원회장과 상원의 마리아 캔트웰(Maria Cantwell) 상업과학교통위원회장은 최초의 연방차원의 개인정보 보호법인 미 프라이버시 권리법(American Privacy Rights Act, APRA) 제정 추진에 합의('24.4.7.)

- APRA는 '22년 6월 프랭크 팔론(Frank Pallone) 하원의원이 발의한 데이터 프라이버시 보호법(안)(American Data Privacy and Protection Act, ADPPA)을 기반으로 작성됨
 - 동 법안은 하원 주도로 발의되었으나, 주 개인정보 보호법을 무효화 할 것이라는 일부 주(州), 상원의원의 반대에 부딪혀 의회에서 계류 중인 상태였음
- APRA 제정 목적은 주(州)별로 상이한 개인정보 보호법을 일반법으로 제정함으로써 연방 차원에서 포괄적으로 규율할 수 있도록 통일된 법체계를 확립하기 위함임
 - 현재 미국의 개인정보보호 관련 법률 체계는 특정 산업, 정보 유형, 주(州)별로 세분화 되어 있어, 연방 차원의 법률 제정을 통해 모든 미국인을 위한 개인정보보호 권리 및 보호장치를 마련하는 것을 목표로 함

- APRA는 ‘법률선택주의’에 따라 연방 법률의 적용을 주법률이나 다른 법률보다 우위로 두고 있으나, 소비자 보호, 직원·학생 개인정보 보호, 개인정보 침해 통지 등을 다루는 현행 주법은 예외로 두고 있음
- 또한, 연방거래위원회(Federal Trade Commission, FTC), 주 법무장관(Attorney General, AG) 소송권을 통해 법규를 위반한 자에게 강력히 책임을 물을 수 있는 집행 메커니즘을 구축

2. APRA 주요 내용

(1) 적용 범위

Ⅰ 법률 적용대상이 대상정보를 활용하는 방식에 중점을 두고 규제

- **(적용대상, Covered Entity)** ① 단독이나 공동으로 데이터를 수집·처리·보유·전송하는 모든 처리자, ② 미국 독점금지법(FTC 법)의 적용을 받는 기관, 통신법 적용을 받는 일반 통신사업자, 비영리단체(NGO) 등
 - 단, 다음 조건을 충족하는 기관은 적용대상에서 제외
 - ※ (소기업) ① 직전 3년간의 연평균 매출이 4,000만 달러 미만, ② 개인정보 처리 대상이 20만 명 미만, ③ 제3자에게 정보를 판매·제공하지 않는 소기업 등
 - (정부기관) 정부기관 또는 정부기관을 대신하여 정보를 수집·처리·보유·전송하는 기관
 - (사기대응 NGO) 사기(fraud)를 예방·조사하는 것이 주된 업무인 비영리단체
- **(대상정보, Covered Data)** ① 개인 또는 기기를 식별하거나, ② 개인 또는 기기와 연결되거나 ③ 합리적으로 연결될 수 있는 정보를 포함
 - (제외대상) 비식별화된 정보, 직원정보, 공개적으로 이용 가능한 정보, 민감정보에 해당하지 않고 대상정보와 결합되지 않은 여러 공개된 정보를 통해 추론한 정보, 도서관·기록보관소·박물관 컬렉션 정보 등은 제외
 - (민감정보) 정부 식별자, 건강정보, 생체인식정보, 유전정보, 금융 계좌 및 결제정보, 정밀한 위치정보(1,850ft 이하), 로그인 자격 증명, 성생활 관련 정보, 개인 일정 또는 주소록 데이터, 전화기록, 사진·녹음파일, 개인의 나체·사적 부위를 보여주는 매체, 비디오 프로그램 시청 정보, 개인의 인종·민족·국가·종교·성별에 관한 정보, 개인의 온라인 활동과 여러 웹사이트에 걸친 활동을 드러내는 정보, 미성년자에 대한 정보, 기타 FTC가 민감정보로 규정한 정보 등

I 영향력이 큰 소셜 미디어 기업과 대규모 데이터 보유자를 지정하고, 추가적인 의무 부여

- 아래 조건을 충족하고, 온라인 플랫폼을 제공할 경우 ‘영향력이 큰 소셜 미디어 기업(High-Impact Social Media Companies)’으로 지정되며, 사용자의 온라인 활동을 통해 수집한 정보는 민감정보로 구분
 - 연간 글로벌 매출액이 30억 달러 이상(법인 계열사 매출 포함)
 - 직전 12개월 중 최소 3개월 동안 전 세계 월간 이용자 수가 3억 명 이상인 플랫폼 운영
 - 플랫폼 주 사용 목적이 개인이 사용자 제작 콘텐츠에 접근·공유하기 위함일 경우
- 일정 규모 이상의 정보를 수집·처리·보유·전송하며, 최근 매출액이 2억 5,000만 달러 이상인 경우 ‘대규모 데이터 보유자(Large Data Holders)’로 지정
 - 500만 명 이상의 대상정보(개인과 연결될 수 있는 1,500만 개의 휴대용 기기 또는 3,500만 개의 커넥티드 기기)를 수집·처리·보유·전송
 - 20만 명 이상의 대상정보(개인과 연결될 수 있는 30만 개의 휴대용 기기 또는 70만 개의 커넥티드 기기)를 수집·처리·보유·전송
- 영향력이 큰 소셜 미디어 기업과 대규모 데이터 보유자에게 추가적인 의무 부여
 - 지난 10년간 사용한 개인정보 처리방침 각 버전의 사본을 보관하고 웹사이트에 게시
 - 사용자가 주요 변경사항에 따른 영향을 충분히 인지할 수 있도록 지난 10년간 변경된 개인정보 처리방침의 주요 변경사항, 변경일자를 명시한 기록을 웹사이트에 공개
 - 개인정보 처리 절차 및 정보주체 권리에 대해 설명한 약식 통지서(short-form notice)를 500 단어 이하로 간결하고, 명확하고, 쉽게 접근가능한 방식으로 제공해야 함

(2) 데이터 수집·처리 최소화 원칙

I APRA는 EU의 GDPR, 한국 개인정보 보호법과 동일하게 개인정보 처리 목적에 필요한 최소한의 개인정보만 처리하도록 제한하는 ‘개인정보 최소화 원칙’을 기반으로 함

- 적용대상 기관 또는 개인정보 수탁자는 개인이 요청한 서비스(제품)를 제공하기 위해 처리 목적을 벗어나 정보를 수집·처리·보유·전송하는 것을 금지
- APRA 적용대상 기업·기관은 처리 목적에 근거하여 명시적 동의 없이 민감정보를 수집하거나, 제3자에게 전송할 수 없으나 다음과 같은 상황에서는 예외적으로 허용
 - 정보보안 목적, 법적 의무 준수 목적, 제품 리콜(결함 보상) 또는 보증 이행 목적, 시장 조사 수행, 제품 개선 및 연구 목적으로 데이터를 비식별화 조치하는 경우, 사기 및

괴롭힘 방지, 진행 중이거나 보안 사고 예방, 공공 안전 사고에 대응하기 위한 목적, 광고를 위해 민감하지 않은 정보를 처리하는 경우

- 사전 동의 없이 생체정보 및 유전자 정보를 수집·전송할 수 있는 처리 범위는 제한적이므로 명시적인 동의 수집 필요

(3) 인공지능 관련 의무사항

Ⅰ 인공지능과 관련하여 APRA 우선 적용, 알고리즘 영향평가 등 의무화

- **(선점원칙)** 인공지능이 생성한 이미지 및 사적인 이미지(intimate images)*에 대해 주(州) 법에 앞서 APRA를 우선 적용
 - * 사적인 이미지(intimate image) : 성적으로 노골적인 이미지 등 개인의 사적인 영역이 담긴 이미지 또는 동영상
- **(대상 알고리즘, Covered Algorithm)** 인공지능이 대상정보를 활용하여 제품 또는 서비스 제공을 결정하거나, 정보를 개인에게 제공하거나 표시하는 순위·정렬·홍보·추천 등을 통해 의사결정을 용이하게 하는 절차를 ‘대상 알고리즘’으로 정의하고 다음과 같은 의무 부여
 - 중대한 위험을 초래할 수 있는 방식으로 대상 알고리즘을 사용하는 대규모 정보 보유자는 알고리즘 영향평가를 실시하도록 의무화하고, 평가 결과를 FTC에 제공 및 공개
 - ※ 영향평가 범위 : ▲ 알고리즘 설계 과정, 방법론, 목적 ▲ 알고리즘이 사용하는 데이터, 특정 데이터의 범주, 모델 학습에 필요한 데이터 등 ▲ 알고리즘이 생성하는 출력물에 대한 설명 ▲ 처리 목적에 따른 알고리즘의 필요성 ▲ 알고리즘에 따른 잠재적 위험성 완화를 위한 조치 또는 향후 조치할 사항에 대한 설명
 - 인공지능에 대한 잠재적 위험성을 줄이기 위해 알고리즘을 배포하기 전 설계 평가를 실시하고, 평가 결과를 연방거래위원회(FTC)에 제공 및 공개
 - 대상 알고리즘이 의사결정*에 사용되는 경우 이를 통지하고, 정보주체가 해당 알고리즘 사용을 거부할 수 있는 권리(Opt-Out)를 제공
 - * 개인의 주택, 고용, 교육, 의료, 보험, 신용 또는 공공시설 이용 및 향유와 관련된 결정

(4) 데이터 브로커 관련 의무사항

Ⅰ 데이터 브로커임을 웹 사이트에 공개, 정보주체 권리보장 도구 제공 등 의무화

- **(데이터 브로커, Data Broker)** 대상정보를 직접 수집하지 않고, 대상정보의 처리나 전송을 통해 수익을 얻는 기업기관으로 다음과 같은 내용을 포함해 웹사이트를 공개적으로 운영할 의무 부여
 - 웹 사이트에 데이터 브로커임을 표시
 - 정보주체가 자신의 개인정보를 삭제하고 처리 중단을 요청할 권리(Opt-Out)와 권리보장을 행사할 수 있는 도구 제공

- 데이터 브로커 등록 여부를 확인하기 위해 FTC가 제공하는 '데이터 브로커 레지스트리(등록정보)' 사이트로 연결되는 링크를 안내해야하며, 추후 콘텐츠에 관한 지침을 마련하도록 규정
 - ※ APRA는 FTC가 데이터 브로커 규정하고 있으며, 5,000명 이상의 개인정보를 처리·전송하는 데이터 브로커는 매년 등록해야 함
- 데이터 브로커가 스토킹 또는 괴롭힘, 사기 목적 등으로 대상정보를 활용하거나 사업과 관련된 사항을 허위로 표시하는 행위를 금지

(5) 애드테크 관련 의무사항

Ⅰ 이용자들에게 맞춤형 광고를 거부할 수 있는 권리를 알려야 함

- (애드테크, AdTech) 개인의 선호도, 관심사항을 기반으로 온라인 광고를 노출하는 기술로, APRA는 정보주체의 권리 중 하나로 맞춤형 광고를 거부할 수 있는 권리를 인정하고 있음
 - 개인의 온라인 활동 및 여러 웹사이트에 걸친 활동을 드러내는 정보 등을 민감정보로 포함하고 있어 명시적인 동의 없이 17세 미만의 어린이를 대상으로 한 맞춤형 광고를 금지하도록 함

(6) 사적 소송권

Ⅰ 개인이 APRA 위반 혐의에 대해 적용대상 기관을 상대로 소송을 제기할 수 있는 권리 보장

- 개인은 개인정보 침해 관련 건뿐만 아니라 APRA 조항 위반에 대해서도 민사 소송을 제기할 수 있음
 - 개인은 특정 기업이 민감정보를 처리하는 것에 대해 APRA에서 요구하는 명시적인 동의 기준을 충족하지 않을 경우 소송 제기 가능
- 위반행위로 인해 중대한 프라이버시 침해*가 발생하지 않는 한, 소송을 시작하기에 앞서 30일간 위반사항을 바로잡는 기간(교정기간)을 가질 것을 규정하고 있음
 - * 1만 달러 이상의 금전적 피해, 의료 환경에서 개인에 대한 신체적 또는 정신적 피해, 피해가 예상되는 공격적인 침해 또는 보호받는 특성에 대한 차별 등으로 정의
- 단, 중대한 프라이버시 침해로 인한 소송 청구 또는 미성년자 관련 위반사항에 대해서는 교정기간을 가질 수 없음

(7) 집행 및 감독

Ⅰ APRA를 집행할 수 있는 권한을 FTC와 각 주의 법무장관(AG)에게 부여

- (FTC) APRA의 집행권한의 우선권은 FTC에 있으며, APRA에 의거한 권한 행사 및 업무 수행을 위해 FTC 산하에 APRA 집행을 담당하는 국을 신설해야 함
 - APRA의 위반은 불공정하거나 기만적인 관행을 규정하는 FTC 규칙을 위반한 것으로 간주
 - FTC는 소비자 구제를 위해 '개인정보 및 보안 피해자 구제기금을 조성해야 함
 - FTC가 APRA 집행 및 관리에 내용을 상세히 작성하여 연방 의회에 제출할 것을 규정
- (법무장관, AG) APRA는 각 주의 법무장관, 최고 소비자 보호 책임자 및 기타 주 공무원에게 연방 지방법원에서 APRA를 집행할 수 있는 권한 부여
 - 각 주에서는 금지명령, 민사 벌금, 손해배상 및 소비자 보상, 변호사 수임료 및 기타 소송 비용, 구제방안 등을 요구할 수 있음
 - 주 법무장관들은 APRA에 의거한 소송 절차를 개시하기 전 FTC에 통지해야 함

(8) 개인정보보호 강화 기술 파일럿 프로그램

Ⅰ APRA는 기업이 개인정보보호 강화 기술(Privacy Enhancing Technologies, PET)를 배포할 수 있도록 FTC가 파일럿 프로그램을 운영할 것을 명시하고 있음

- 적용대상 기관은 APRA의 정보 보안 요건을 충족하는 특정 PET를 채택할 수 있음
- 파일럿 프로그램에 참여하는 기업에게는 개인정보 침해와 관련한 사적 소송에서 해당 PET의 채택을 통해 APRA의 정보 보안 요건 준수를 입증할 수 있는 자격을 부여

3. 결론 및 시사점

Ⅰ APRA가 제정될 경우 현재 시행 중인 주(州) 별 개인정보 보호법보다 우선 적용됨으로써 미국 전역에 포괄적이고 일관된 개인정보보호 의무 및 규율체계 제공 가능

- 연방 의회와는 별도로 미국 연방거래위원회(FTC)도 자체적으로 개인정보보호를 수행하는 법 집행 감독기관으로써의 역할을 담당하고자 개인정보보호에 관한 FTC 규칙을 제정하고 있음

I 인공지능 알고리즘을 적용하여 자동화된 의사결정을 활용하는 기업에 대한 법적 의무를 부과하는 등 일부 측면을 규제하고 있음

- 알고리즘을 활용하는 기업들은 잠재적 피해 위험을 최소화하기 위해 AI 모델의 영향을 평가하고 개인정보 보호 기반의 설계 방식을 도입할 필요가 있음
- 데이터 최소화 원칙으로 인해 인공지능 학습에 필요한 데이터를 제한할 수도 있다는 우려도 존재

I 선점주의 조항과 사적 소송권 관련 조항에 대해 주 정부와 이해관계자들이 반대하고 있어, 법률 제정에 필요한 초당파적 지지를 얻기 위한 합의 필요

- 현재 미국 14개주 및 컬럼비아 특별구(Washington D.C.)의 법무장관들은 공개된 APRA 초안의 일부 조항에 반대하는 서한을 연방정부에 전달한 상태('24.5.8.)
 - ※ 반대 서한에 서명한 주는 컬럼비아 특별구 외에 캘리포니아, 코네티컷, 델라웨어, 하와이, 일리노이, 메인, 매사추세츠, 메릴랜드, 미네소타, 네바다, 뉴욕, 오리건, 펜실베이니아, 버몬트 등을 포함
- APRA의 선점주의 조항이 '18년 이후 각 주에서 제정한 포괄적 개인정보 보호법을 무효화할 것이라는 우려에서 제기
- 특히 캘리포니아주 개인정보 보호법의 경우 옵트아웃(opt-out) 요건 및 위험평가 요건을 규정하는 등 APRA나 다른 주법에서 요구하는 수준 이상으로 의무사항을 설정했기에, 연방법이 우선 적용될 경우 개인정보보호 규제가 약화할 수 있다는 우려 존재
- 반대 서한은 주 정부가 개인정보보호의 영역에서 연방정부의 선점을 반대하는 활동을 지속할 것임을 시사
 - 적용대상 기관들은 미국 내 개인정보보호 규제의 변화 추이를 모니터링하고, 법적 요구사항을 파악하여 위반사항이 발생하지 않도록 지속적인 노력 필요

출처 |

1. Congressional Research Service, The American Privacy Rights Act, 2024.5.7.
2. Dataguidance, USA: American Privacy Rights Act - what you need to know, 2024.4.
3. JDSUPRA, Here We Go Again: Another Attempt at a Comprehensive Federal Data Privacy Law, 2024.5.21.
4. White & Case, Proposed American Privacy Rights Act seeks to establish a comprehensive national framework for data privacy, 2024.4.18.
5. 개인정보보호위원회, 미국 여·야, 빅테크 규제 위해 연방 개인정보보호 법안 합의, 2024.4.24.
6. 대륙아주, 美 국회 상·하원, 자국민의 개인정보를 무분별하게 수집·활용하는 것을 막기 위한 연방 차원의 포괄적 개인정보보호법인 '미국 프라이버시 권리법' (American Privacy Rights Act of 2024) 법안에 합의, 2024.5.9.

EDPS 2023 연례보고서 분석



[목 차]

1. 개요

2. '23년 EDPS의 주요 활동

- (1) 감독 및 집행
- (2) 정책 및 자문
- (3) 기술 및 개인정보보호

3. '24년 EDPS의 비전 및 목표

4. 결론 및 전망

1. 개요

■ 유럽 개인정보보호 감독관(European Data Protection Supervisor, EDPS)은 유럽연합의 일관된 개인 정보보호를 보장하기 위해 회원국의 개인정보 감독기구(Data Protection Authority, DPA)와 협력하는 독립적인 감독기구로서 개인정보 관련 감독 및 집행, 정책 자문 등의 업무 수행

- (감독 및 집행) EU 기관 및 기구들(European Institutions, agencies and bodies, EUI)의 개인정보 처리를 감독
- (정책 및 자문) 개인정보보호 관련 정책 및 법률안에 대해 자문
- (기술 및 프라이버시) 개인정보보호 관련 기술개발을 모니터링 및 평가하고, EUI 개인정보 처리시스템의 보안조치의 실행을 관리·감독
- (협력) 유럽 개인정보 감독기구(DPA)와 협력하여 EU 및 유럽 경제 지역(European Economic Area, EEA) 전체에서의 일관된 개인정보보호를 촉진

■ '23년은 진화하는 디지털 발전과 규제 환경에 대한 EDPS의 적응력과 개인정보보호 기준 향상을 위해 다자간 및 국경 간 협력의 중요성을 입증한 해였다고 평가

- '24년 4월 EDPS가 발표한 '2023년 연례보고서([EDPS Annual Report 2023](#))'는 '23년 EDPS의 주요 활동 내역과 EDPS의 '24년 비전 및 목표를 제시

2. '23년 EDPS의 주요 활동

(1) 감독 및 집행

Ⅰ EDPS는 EUI가 개인정보를 처리하는 방식을 지속적으로 모니터링, 안내 및 검증하여 데이터 보호 규정(EUDPR*)을 준수하는지 확인

- * EUDPR(European Data Protection Regulation, Regulation (EU) 2018/1725) : EU의 입법기관(institutions), 자문·감사·감독·외교기관(bodies), 지원기관(offices), 정책집행기관(agencies)이 개인정보를 처리하는 방식을 규정
- 개인정보 처리에 대해 EUI에 조언하는 ① 감독 의견서(Supervisory Opinions) 발행, ② 침해 또는 불만이 제기된 후 규정 준수 여부를 확인하기 위한 조사 및 감사 수행, ③ EUI 개인정보보호 책임자와 협력하여 개인정보보호 문화 정착화 등의 업무를 수행

Ⅰ ① 감독 의견서 발행

- EDPS의 감독 의견서는 일반적으로 EUI가 업무에서 개인정보를 처리하는 방식에 대해 EDPS 주도하거나, EU 집행위원회(European Commission)의 요청에 의해 발행
- '23년에 EDPS는 총 15개의 감독 의견서 발표
 - EUI 또는 EU 회원국 간의 정보 교환, 생체인식정보 처리, 다양한 목적의 소셜 미디어 사용, 컨트롤러(controller)-프로세서(processor) 관계성¹⁾ 등의 주제를 다루고 있음

1) 컨트롤러는 개인정보 처리의 목적과 수단을 결정하고 프로세서는 컨트롤러를 대신하여 업무를 처리하는데, 여러 명의 컨트롤러와 프로세서가 개인정보 처리에 대한 책임을 공유하는 경우 공동 컨트롤러 및 공동 프로세서라고 함

표 1 '23년 EDPS 감독 의견서 발행 내역

발행 시기		내용
1	'23.1.11.	유로폴(Europol) 규칙 제11조제(1)항제(q)호, 제18호, 제18a조에 의거해 채택된 유로폴 이사회 결정 관련
2	'23.3.20.	유럽노동청(European Labour Authority, ELA)의 DPO 관련 시행 규칙 초안 관련
3	'23.4.4.	개인정보 처리와 관련하여 특정 정보주체 권리의 제한에 관한 EIT의 내부 규칙 관련
4	'23.5.11.	유럽 의회 의원(Member of the European Parliament, MEP) 생체인식 출석 등록(biometric attendance register) 관련
5	'23.5.11.	국경 간 범죄 용의자 식별을 목적으로 유럽 국경 및 해안 경비대(FRONTEx)에서 처리하는 개인정보 관련
6	'23.5.31.	EU 이사회 사무국(General Secretariat of the Council, GSC)의 중앙 집중식 인적 자원 분석 및 보고 서비스 프로젝트와 데이터 웨어하우스 구축 관련
7	'23.6.13.	EU 집행위원회의 공통 보존 목록(common retention list)의 세 번째 개정 관련
8	'23.6.19.	개인정보 처리 맥락에서 특정 정보주체 권리의 제한에 관한 글로벌 보건 유럽 및 개발도상국 임상시험 파트너십 3 공동사업 (EDCTP3)의 내부 규칙 관련
9	'23.6.19.	특정 도구 및 서비스(HAN/AREs)의 사용과 관련하여 집행 기관 ²⁾ 과 EU 집행위원회 간 개인정보보호 책임 공유 관련
10	'23.6.19.	개인정보 처리 맥락에서 특정 정보주체 권리의 제한에 관한 스마트 네트워크 및 서비스 공동 사업(SNS)의 내부 규칙 초안 관련
11	'23.6.26.	개인정보 처리 맥락에서 특정 정보주체 권리의 제한에 관한 유럽 사이버보안 산업, 기술, 연구 역량 센터(European Cybersecurity Competence Centre, ECCC) 내부 규칙 초안 관련
12	'23.6.27.	사회보장정보의 전자적 교환(Electronic Exchange of Social Security Information, EESSI) 프로젝트 맥락에서 개인정보 처리와 관련한 유럽 위원회의 역할 관련
13	'23.6.28.	EUI와 체결한 서비스 수준 계약에서 EU 집행위원회의 급여 관리자 사무실(Paymaster Office, PMO)의 지위 관련
14	'23.10.13.	괴롭힘 예방 및 퇴치에 관한 위원회 결정 초안 및 특정 개인정보 주체의 권리 제한에 관한 위원회 결정 초안 관련
15	'23.11.9.	유럽질병예방통제센터(European Centre for Disease Prevention and Control, ECDC)의 전염병 인텔리전스 목적의 소셜미디어 모니터링 사용 관련

출처 : Supervisory Opinions(EDPS, 2024)³⁾

2) 유럽 기후·인프라·환경집행청(CINEA), 유럽 교육·문화집행청(EACEA), 유럽 혁신위원회·중소기업집행청(EISMEA), 유럽 연구위원회집행청(ERCEA), 유럽 보건·디지털집행청(HaDEA) 및 유럽 연구집행청(REA) 등을 포함

3) https://www.edps.europa.eu/data-protection/our-work/our-work-by-type/supervisory-opinions_en 참고

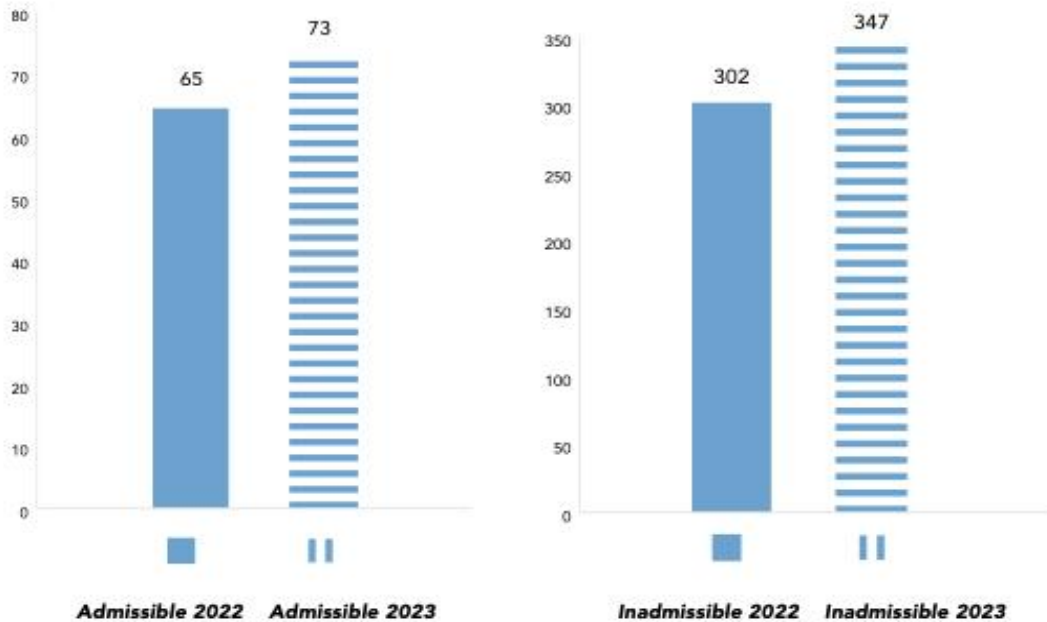
I ② 조사(Investigations)

- '23년에는 EUI가 데이터 보호 규정(EUDPR)을 위반했는지를 효과적으로 확인하기 위해 조사 절차 개선
 - 개선된 조사절차는 '조사 개시 → 증거 수집 회의 → 현장 또는 원격 조사 → 예비 평가 → 청문회(선택사항) → EDPS의 최종 결정 및 공표 → 시정조치' 순
- '23년에 진행한 조사는 EU 또는 유럽 경제 지역(EEA) 외부로 개인정보를 전송할 수 있는 EUI의 IT 도구 및 클라우드 서비스 사용 등에 대한 조사 내용을 다룸
 - '23년 EUI의 웹사이트와 관련해 5건의 민원을 기반으로 조사를 수행했으며, 최종 결정은 '24년에 내릴 예정
 - 오랫동안 지속된 데이터 침해, 다수의 개인에게 영향을 준 데이터 침해, EUI와 관련되어 있거나 CERT-EU가 지정한 사이버 공격으로 인해 발생한 데이터 침해 등에 대한 조사 및 후속조치 시행

I ③ 감사(Audits)

- EUI가 EUDPR을 어떻게 실행하고 있는지 확인하는 감사를 지속적으로 수행
 - '23년에는 유럽인사선발사무소(European Personal Selection Office, EPSO)와 유럽투자은행(European Investment Bank)을 대상으로 감사 수행
 - EDPS가 수행하는 감사에 대한 위험평가 방법이 적절하게 설계되고 구현되는지에 대해 유럽공동체(EC)의 내부 감사 서비스 수행
- EDPS에 접수되는 민원 수가 증가하여, 개인에게 신속한 답변 제공을 위해 민원 페이지 개편
 - 개인정보에 대한 정보주체의 접근권, 삭제권, 개인정보 보관 등과 관련한 민원이 상당수를 차지
 - 홈페이지 개편을 통해 민원과 관련한 EDPS의 권한, 민원 제출 방법 등 사용자들이 쉽게 이용할 수 있도록 환경 개선
- EDPS는 데이터 보호 담당자의 역량 강화를 위해 EUI의 개인정보보호 책임자(data protection officers, 이하 DPO)에게 조언을 제공하고, 각 EUI가 규정 EUDPR 요건을 준수하며 독립적인 협의체를 구성할 수 있도록 지원
 - 대표적으로 EDPS-DPO 회의, DPO 지원 그룹, DPO 대상 원탁회의 등을 추진하여 지속 가능한 협력관계를 구축하고자 노력

그림 1 EDPS 민원 접수 건수 증가 추이('23~'24)



출처 : EDPS ANNUAL REPORT 2023(EDPS, 2024.4.9.)

(2) 정책 및 자문

Ⅰ 개인정보보호 관련 법안에 대하여 EU의 공동 입법기관(EU 집행위원회, 유럽의회, EU 이사회)에 자문 역할 수행

- EDPS는 '23년 한 해동안 의견서(Opinion), EU 개인정보보호이사회(European Data Protection Board, EDPB)와의 공동 의견(Joint Opinion), 공식·비공식 코멘트 등의 다양한 형태로 총 116건의 입법 자문 제공
 - 인공지능(AI), 금융, 법무 및 내무 분야 등 다양한 주제에 대한 자문 수행
- (인공지능) 인공지능법(안)(AI Act)과 관련하여 EU의 공동 입법자들에게 인공지능 도구와 시스템의 개발이 EU의 개인정보보호 법적 요건을 준수하도록 조언하고, 사용하는 AI 시스템으로 인해 개인에게 지나친 위험을 초래하는 경우 사용을 금지하는 것을 강조
 - EU 정보기관이 사용하는 AI 시스템으로 인해 피해를 입은 개인이 다른 EU 회원국의 민간 또는 공공 부문에서 사용하는 AI 시스템으로 인해 피해를 입은 개인과 동일한 방식으로 보호받을 수 있도록 AI 책임 규정에 대한 자문도 제공

- (금융) 개인정보의 중앙 집중화 및 과도한 처리를 방지, 최고 수준의 개인정보보호 등을 위해 디지털 유로* 및 금융 및 결제 서비스 관련 입법 제안에 노력
* 디지털 유로 : 현금 외 추가적인 결제 수단으로 온온프라인에서 전자 결제를 할 수 있는 기능 제공
- (법무 및 내무 분야) 이동의 자유, 안보 등 EU 시민의 권리 보호 및 개인정보 처리와 관련된 문제에 대한 입법을 위해 EU 공동 입법자에게 자문 제공

Ⅰ 유럽 내외 관련 기관과의 지속적인 협력을 통해 정보 및 모범 사례 교환

- (EDPB와의 협력) EU와 동일한 수준으로 데이터를 관리하기 위해 유럽 경제지역(EEA) 외부로 데이터를 전송하거나 특정 소셜 미디어 플랫폼의 데이터 처리 등에 대해 EDPB와 지속적으로 협력하여 자문 제공
- (국제 협력) EU 개인정보보호 표준의 글로벌화를 지원하고자 글로벌 개인정보보호 총회(Global Privacy Assembly), 프라이버시 감독기관들과의 G7 원탁회의 등을 통해 국제 파트너와 긴밀히 협력하고 있으며, 이 과정에서 생성형 AI에 대한 결의안을 채택

(3) 기술 및 개인정보 보호

Ⅰ 미래 기술이 개인정보보호 및 데이터 보호에 미치는 영향을 평가하고 기술 환경 변화를 대비하기 위한 역량 강화

- EDPS의 기술 및 개인정보보호 부서(Technology and Privacy Unit)는 전문성을 위해 ① 기술 모니터링과 예측, ② 디지털 전환, ③ 시스템 감독 및 기술 감사의 세 가지 부문을 중심으로 조직 구성

Ⅰ ① (기술 모니터링과 예측) 예측 기반 접근 방식을 사용하여 기술 개발을 모니터링

- (TechSonar 보고서) 개인정보보호에 대한 전략적 예측, 예측과 미래 연구 간 격차 해소를 위한 유럽 최초의 이니셔티브인 TechSonar 보고서를 통해 미래의 기술적 과제 해결
 - 대규모 언어 모델(LLM), 디지털 신원 지갑, 행동 인터넷(loB)*, 확장 현실, 딥페이크 탐지 등을 중점으로 연구
 - * 행동 인터넷(Internet of Behaviors, loB) : 사물인터넷(IoT) 각 디바이스에 IP 주소가 있는 것과 동일한 방식으로 개인의 행동 패턴을 디지털로 추적하고 분석하여 이에 대한 인사이트를 얻는 개념
 - 기술이 개인에게 미칠 수 있는 긍정적 측면, 개인정보보호 관련 과제 및 영향, 개인정보 및 데이터 보호에 관한 정보주체의 권리에 대해 조사

- (TechDispatch) TechSonar를 통해 미래 기술 동향과 미치는 영향을 예측하였고, TechDispatch의 강연과 보고서를 통해 기술 개발, 개인정보 및 데이터 보호에 미치는 영향을 모니터링
 - '23년에는 유럽중앙은행(European Central Bank)이 추진하고 있는 디지털 화폐와 설명 가능한 인공지능(Explainable Artificial Intelligence)에 중점을 둠
- (The Internet Privacy Engineering Network, IPEN) 다양한 전문가들이 모여 신기술이 개인정보보호에 미치는 영향에 대해 논의하는 플랫폼인 IPEN 워크숍을 주최
- (기술 분야 국제협력) 디지털 및 규제 환경이 발전함에 따라 개인정보 및 데이터 보호 문제에 대해 전문성을 확장하고 정보 제공을 위한 국제 파트너와 협력체계 구축
 - EDPB와 개인정보의 익명화, 가명화 및 기타 기술적 측면(예: ePrivacy Directive와 같은 특정 개인정보보호 규제를 해석하는 방법)에 대해 긴밀히 협력하는 것을 포함
 - 국제 실무그룹과 글로벌 개인정보보호 총회(Global Privacy Assembly)와 협력하여 개인정보 및 데이터 보호에 대한 기술 공유

Ⅱ ② (디지털 전환) 무료 오픈소스 소프트웨어 탐색과 배포

- 통신 및 소프트웨어 서비스 제공업체에 대한 의존도를 최소화하여 구속 현상(Detrimental Lock-in)을 예방하고자 무료 오픈소스 소프트웨어 및 솔루션을 탐색하여 배포
 - '23년 IT 관련 요구사항 파악을 위해 자체 IT 타당성 조사 수행, EDPS 자체 클라우드 출시, 이미지 및 비디오 공유 채널인 'EU 보이스' 및 'EU 비디오' 등 운영
- 디지털 전환을 위해 신뢰할 수 있는 eIDAS* 제공업체로부터 디지털 서명을 조달하고 설치하여 EDPS에서 서명한 디지털 문서에 최고 수준의 무결성, 인증, 부인 방지 기능 제공
 - * eIDAS : 전자 거래를 위한 전자 식별 및 신뢰 서비스를 관리하기 위한 EU 규정으로, 안전한 형태의 전자 식별 체계를 사용하여 안전하고 원활한 전자 상호 작용을 가능하게 함

Ⅱ ③ (시스템 감독 및 기술 감사) 대규모 IT 시스템 감사와 개인정보 유출 관리 등을 담당

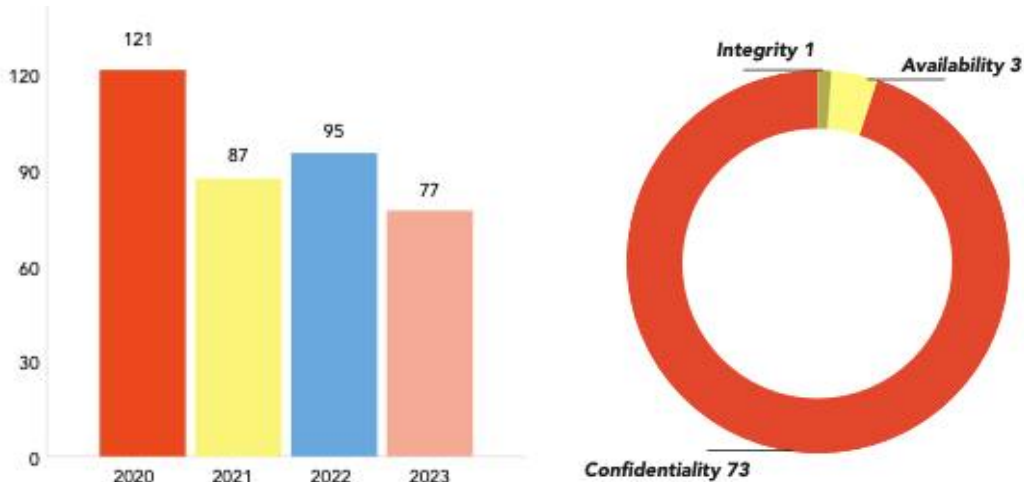
- EDPS의 시스템 및 기술 감사 부문은 대규모 IT 시스템을 운영하는 EUI가 법을 준수하고 개인정보를 보호하는데 필요한 기술적 조치를 취했는지 관리·감독
 - (감사) '23년에는 EU 법률과 관련된 정보를 교환하는 내부 시장 정보시스템(IMI)의 개인정보보호 관행, EU의 대규모 IT 시스템 운영관리 기관(eu-LISA)가 관리하는 쉥겐 정보 시스템(Schengen Information System)⁴⁾의 보안 정책 및 관리체계에 대해 감사 수행

4) 쉥겐 정보 시스템은 쉥겐 회원국(벨기에, 네덜란드, 핀란드 등 27개국) 간 국경 통제 및 법 집행 협력을 지원하는 대규모 정보 공유 시스템으로 EDPS는 국제 감사 기준에 따라 최소 4년 마다 개인정보 처리에 대한 감사를 수행해야 함

- (개인정보 침해) EU 데이터 보호 규정(EUDPR)에 근거하여 EUI가 '23년 EDPS에 통지한 개인정보 침해 건수는 77건이었으며, 기밀성 침해가 73건, 무결성 침해는 1건, 가용성 침해는 3건이었음

※ 제출된 77건의 데이터 침해 통지 중 5건은 모든 유형의 침해가 복합적으로 발생

그림 2 '23년 개인정보 침해 통지 건수 및 침해 유형



출처 : EDPS ANNUAL REPORT 2023(EDPS, 2024.4.9.)

EDPS는 핵심 성과지표(KPI)를 통해 주요 목표를 수립하고 성과를 모니터링하여 업무의 영향력을 높이고 자원을 효과적으로 사용

표 2 '23년 EDPS 주요 활동 지표(KPI) 목표 및 실적

	KPI	지표 설명	'23년 목표	'23년 실적
1	내부지표	EDPS가 주관하거나 공동 주관한 기술 모니터링 및 개인정보 및 데이터 보호 강화를 위한 기술 홍보 관련 사례(출판물 포함) 수	10건	20건
2	내부 & 외부지표	분야 간 정책 솔루션에 초점을 맞춘 활동 수(내부 및 외부)	8회	8회
3	내부지표	EDPS가 상당한 서면 기고를 제공한 국제 협력(GPA, CoE, OECD, GPEN, IWGDPT, 춘계 컨퍼런스, 국제기구)의 맥락에서 다루어진 사례 수	5건	36건

4	외부지표	EDPS가 EDPB의 맥락에서 수석 보고자, 보고자 또는 초안 작성 팀의 일원으로 활동한 파일 수	5개	20개
5	외부지표	유럽연합 집행위원회의 입법 자문 요청에 대한 응답으로 발행된 제42조 의견서 및 공동 EDPS-EDPB 의견서 수	전년도 기준	56개 의견
6	외부지표	물리적 또는 원격으로 수행된 감사/방문 횟수	5회	9회
7	외부지표	EDPS 소셜미디어 계정의 팔로워 수	전년도 팔로워 수 대비 10% 증가	X: 29,413명 LinkedIn: 71,238명 EUVoice: 5,906명 EUVideo: 752명 YouTube: 2,984명 총: 110,293명

출처 : EDPS ANNUAL REPORT 2023(EDPS, 2024.4.9.)

3. '24년 EDPS의 비전 및 목표

I EDPS는 '24년에 20주년을 맞이하여 개인정보보호 환경 개선과 향후 과제를 발굴하기 위한 목표 수립

- EDPS는 개인정보보호의 중요성과 영향력을 강조하기 위한 네 가지 핵심 목표(Key pillars)를 설정
 - (Pillar 1) 지난 20년간의 개인정보보호 활동과 EDPS의 영향력을 웹 사이트에 게시하고, 데이터 보호에 관한 미래 지향적인 분석 보고서 제작
 - (Pillar 2) 프라이버시 보호가 각 분야에서 어떻게 진행되고 있는지 공유하기 위해 전 세계 주요 인사들과 20번에 걸친 회담 진행
 - (Pillar 3) 개인의 기본권을 더욱 강화하기 위한 20개의 이니셔티브를 추진함으로써 미래 대응을 위한 EDPS 접근방식 현대화
 - (Pillar 4) '24년 6월 벨기에 브뤼셀에서 열리는 '유럽 개인정보 보호 서밋(European Data Protection Summit – Rethinking Data in a Democratic Society)' 에서 현대 민주주의에서의 프라이버시 보호를 위한 역할 등에 대한 토론 수행

4. 결론 및 전망

- '23년도 연례보고서를 통해 EDPS에서 수행한 감독 및 집행, 정책 자문, 기술 등 개인정보보호를 위한 주요 활동 사항을 공개
- '23년 한 해 동안 인공지능이 화두가 됨에 따라, EDPS는 개인정보 및 데이터 보호에 대한 기본권을 중심으로 인공지능 도구의 개발, 적용을 위한 규칙·원칙을 제시함으로써 AI 발전에 기여
 - 개인정보보호 및 프라이버시 감독기관들과의 G7 원탁회의에서 생성형 AI에 관한 성명서 채택, 생성형 AI 시스템에 관한 제45차 세계 개인정보보호 총회 결의안 지원 등을 통해 다양한 국제 포럼 및 이니셔티브에서 인공지능 관련 논의를 주도해옴
 - EU의 AI 법안 설계 과정에 적극적으로 참여함으로써 AI 시스템의 개발 및 배포 시 개인정보 보호법을 준수하고 개인의 기본권을 존중할 수 있도록 보장하는 역할을 수행

출처 |

1. EDPS, ANNUAL REPORT 2023, 2024.4.9.
2. EDPS, ANNUAL REPORT 2023 – Executive Summary, 2024.4.9.

2024

개인정보보호 월간동향분석

발간 목록

No.	호수	제목
1	1월 1호	EU 데이터법(Data Act) 주요 내용 분석 및 시사점
2	1월 2호	EU 내 메타의 무광고 유료 서비스 모델의 개인정보 침해 이슈 분석
3	2월 1호	미국 주(州) 개인정보 보호법에 대한 평가 및 분석
4	2월 2호	DPO지정 및 역할에 대한 CEA 2023 조사 분석
5	3월 1호	미국 백악관의 정부 데이터 및 민감 개인정보보호를 위한 행정명령 분석
6	3월 2호	EDPB, GDPR 주 사업장에 관한 성명 발표
7	4월 1호	생체인식정보에 대한 개인정보보호 이슈
8	4월 2호	미국 AI 에듀테크 시장 관련 개인정보보호 규제 현황 및 고려사항
9	5월 1호	미국 연방 개인정보 보호법(APRA) 주요 내용 분석
10	5월 2호	EDPS 2023 연례보고서 분석

2024

개인정보보호 월간동향분석

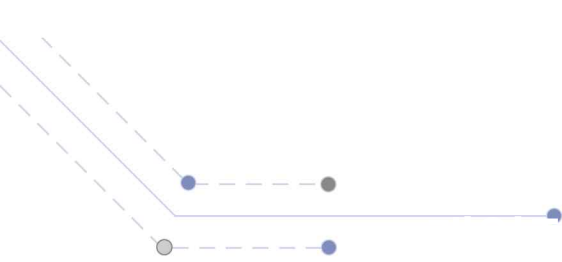
『2024 개인정보보호 월간동향분석 보고서』는
개인정보보호위원회 출연금으로 수행한
사업의 결과물입니다.

한국인터넷진흥원의 승인 없이 본 보고서의 무단전재나
복제를 금하며, 인용하실 때는 반드시
『2024 개인정보보호 월간동향 분석 보고서』라고
밝혀주시기 바랍니다.

본 보고서의 내용은
한국인터넷진흥원의 공식 견해가 아님을 알려드립니다.

발행

발행일 2024년 5월 28일
발행처 한국인터넷진흥원 개인정보정책팀
전라남도 나주시 진흥길 9
Tel : 061-820-1674



2024 개인정보보호 월간동향분석

2024 Vol.5

PRiVACY REPORT

