2023 Privacy Report

개인정보보호 월간동향분석

제1호

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2023 Privacy Report

개인정보보호 월간동향분석

제1호

1. 주요국 개인정보보호 강화기술 정책동향 분석 및 시사점

2. EU 인공지능법(안)과 GDPR의 상호작용 분석

3. 해외 아동 개인정보 침해 관련 행정처분 사례 분석

KISA

주요국 개인정보보호 강화기술 정책동향 분석 및 시사점

[목 차]

1. 개요

▶ 최근 민간과 공공 분야에서 개인정보 가치의 중요성이 크게 강조됨과 동시에 개인정보보호 강화기술(PET, Privacy Enhancing Technology)에 대한 시장 및 정책 측면의 관심이 높아지고 있음

- PET는 개인정보 최소화, 익명화 및 가명화와 기타 핵심적인 프라이버시 및 개인정보보호 원칙을 지원하기 위해 고안된 다양한 유형의 기술을 의미[1)]

- 최근 PET의 시장 출시를 위한 기술 환경이 한층 성숙되고 있는 가운데, OECD와 MIT가 공동으로 실시한 PET 확산 연구[2)]에 따르면, 차등 개인정보보호, 다자간 컴퓨팅, 동형 암호화 및 연합학습 등 PET 기술의 개발 성숙도가 진전됨에 따라 본격적인 시장 수요가 발생 중인 것으로 확인
  - 데이터분석 기반 컨설팅 기업인 DataCo는 PET를 기반으로 예측 모델 성능을 개선하여 다양한 고객 제안에 활용

1) ENISA, https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends/#:~:text=The%20European%20Union%20Agency%20for,privacy%20and%20data%20protection%20principles.
2) IMDA, Invitation to Participate in Privacy Enhancing Technology Sandbox “PET Sandbox”, 2022.7.20. 재인용(p.2)

- 에스토니아의 교육 및 세무 당국은 다자간 컴퓨팅 기술을 기반으로 중복 데이터셋을 활용하여, 중퇴자와 견습생 등록 간의 상관관계를 파악

• 또한, 시장조사기관 Gartner는 '22년 최상위 전략기술 트렌드의 하나로 개인정보보호 강화 컴퓨팅 기술을 지목[3)]

▶ 한편, 도입기 PET 시장에서 기업들은 PET 개발과 관련하여 다음과 같은 애로 사항도 동시에 안고 있음

• PET 솔루션 제공사에 대한 기술 벤치마크가 부족해 적절한 솔루션 제공사를 파악하고 선택하기 어려움

• PET의 기술적 제약 하에서 활용 PET와 활용 사례 요구사항을 구체화하기 위한 방법에 대한 지식이 부족해 PET에 대한 기대 충족이 어려움

• 관련 규제 기관이 규제 대상 데이터의 PET 활용 조건에 관하여 명확한 입장과 기준을 제시하지 않아 기업 등 조직에서 규정 준수 정책 수립이 어려움

▶ 이하에서는 데이터 기반 경제의 촉진을 위한 PET의 활성화를 위한 주요국의 최근 정책 개발 현황을 살펴보고자 함

2. 주요국 PET 관련 지원책 현황

(1) 영국

① PEC 가이던스 초안

▶ 영국 개인정보 감독기구 ICO는 '22.9월, 데이터 보호법의 원만한 적용을 위해 익명화, 가명화 및 PET 적용과 관련된 법률, 정책, 거버넌스 및 기술 이슈를 다룬 보고서 시리즈의 일환으로 PET에 대한 지침 초안[4)]을 개발

• **(배경)** 해당 가이던스 시리즈는 '21.5월 1차 도입부 보고서를 발간한 뒤 '23.1월 시점 총 5권의 보고서[5)]를 공개

3) Gartner, Top Strategic Technology Trends for 2022: Privacy-Enhancing Computation, 2021.10.18
4) Chapter 5: Privacy-enhancing technologies (PETs)- Anonymisation, pseudonymisation, and privacy enhancing technologies guidance. UK ICO, ICO publishes guidance on privacy enhancing technologies, 2022.9.7
5) 보고서별 주제 및 발간 시점- 1차: 제1장 도입('21.5), 2차: 제2장 익명화('21.10), 3차: 가명화('22.2), 4차: 책임성과 거버넌스('22.3), 5차: PET('22.9)

- **(주요 내용)** PET를 다루고 있는 5차 가이던스 초안은 조직이 데이터 보호 내재화(Data Protection by Design)를 통해 데이터의 잠재성 실현을 지원하기 위해 ▲PET의 데이터 보호 준수 ▲위험 및 이점 ▲현재 사용 가능한 PET의 기술 유형 등을 중심으로 작성

  ※ 영국 ICO는 PET를 개인 데이터 사용을 최소화하고 데이터 보안을 극대화하며 개인에게 권한을 부여함으로써 근본적으로 데이터 보호 원칙을 실현하기 위한 기술로, 다양한 기술과 기법을 포괄하는 것으로 정의

- **(위험 요인)** PET 적용에 앞서 의사결정 절차, 데이터 처리의 구체적인 목적 및 정확성과 책임성 요구사항 준수 방안 등에 대한 효과 등을 평가할 필요가 있음
  - (성숙도 부족) 확장성, 표준 활용, 공격 시 견고성 측면에서 PET는 일정 수준의 이상의 기술적인 완성도를 갖추어야 함

    ※ PET 평가와 관련된 요인은 후속 가이던스에서 개발 예정
  - (전문성 부족) PET는 구축 및 적용 시 전문성을 충분히 확보하지 못하면 실행상의 오류나 개인정보보호-활용 간 적절한 균형 달성에 어려움을 겪을 수 있으므로, 이 경우 적절한 지원을 기능한 기성 제품이나 서비스 활용을 검토하는 것이 바람직
  - (실행 오류) 이론과 실제 적용 간의 차이는 개인의 권리와 자유를 침해하는 결과를 초래할 수 있으므로, 공격 및 취약점에 대해 정기적인 모니터링과 적절한 완화 수단 마련이 필요

- **(도입 시 고려사항)** PET를 통해 조직의 목표 달성이 가능할 경우 정보보호영향평가(DPIA)를 실시하여 처리의 특성, 범위, 맥락, 목적, 기술의 완성도 등을 점검해야 함
  - (특성) 개인정보 처리와 관련된 조직의 계획
  - (맥락) 개인정보 처리에 따른 기대에 영향을 미칠 수 있는 내외부 요인이나 처리의 직접적 효과
  - (목적) 개인정보를 처리하고자 하는 이유
  - (기술 완성도) 적용 PET가 조직의 목적을 달성시킬 수 있을 정도로 충분히 성숙한 기술인지 여부와 시장 변화에 따른 PET 관련 정보 업데이트 가능 여부(무작정 최신 기술 채택은 지양)

표1 _ 영국 ICO의 PET 기술 유형별 개요/제공 가치/취약점

기술 유형	개요	제공 가치	취약점
동형 암호(Homomorphic encryption, HE)	암호화된 상태에서 연산을 가능케 하기 위한 기술	보안과 기밀성 연산의 정확성	확장성과 연산 문제 실시간 데이터 분석 취약
안전한 다자간 컴퓨팅(Secure Multiparty Computation, SMPC)	가치를 계산할 수 있는 능력을 제공하는 분산 컴퓨팅 기술로, 개인정보를 타인에게 공개하지 않고 여러 암호화된 데이터 소스에서 입력정보를 수신	보안 데이터 최소화	컴퓨팅 자원 통신 비용

기술 유형	개요	제공 가치	취약점
사적 데이터셋 교차(Private Set Intersection, PSI)	SMPC의 한 유형으로, 각자 고유의 데이터셋을 보유하고 있는 당사자들이 데이터 셋을 공유하지 않고 양측 간의 교차(intersection) 데이터를 확인하기 위한 기술	데이터 최소화	신원 재인식 가능성(과다 분석 및 교차 범위 확장 시)
연합학습 (Federated Learning)	여러 위치에 분산 저장된 데이터를 직접 공유하지 않으면서, 협력하며 AI 학습할 수 있는 분산형 머신러닝 기법	데이터 최소화 적절한 수준의 보안 데이터 침해 위기 최소화	로컬 분석을 위한 표준 포맷 필요 대역 여유 및 컴퓨팅 파워(로컬) 확보 필요
신뢰실행환경 (Trusted Execution Environments, TEE)	메인 프로세서 내 독립된 보안영역(Secure Area)이 제공하기 위한 안전한 실행환경	데이터 유출 보호 데이터 무결성/기밀성 코드 무결성	실행 초기 부채널 공격(side channel attack) 가능성
제로지식증명(Zero-knowledge proofs)	한 당사자(Prover: 증명자)가 다른 당사자(Verifier: 검증자)에게 비밀 자체에 대한 정보를 공개하지 않고 비밀을 소유하고 있음을 증명하기 위한 기술	데이터 최소화 원칙 보안 원칙	취약한 보안 프로토콜 실행 환경 하에서 효과 반감
차등 개인정보보호 (Differential Privacy)	대규모 데이터에서 개별 주체들의 개인정보 노출을 최소화하는 동시에 개인정보를 활용하기 위한 기술	데이터 익명화	프라이버시와 효용성 간의 최적 트레이드오프 설정 어려움
합성데이터 (Synthetic Data)	직접 실제적인 데이터를 확보하지 못하는 특정 상황에 적용가능한 인공적으로 생성된 데이터	데이터 최소화 원칙	통상적 기준을 벗어나는 개인정보 특징 포착 어려움

- 가이던스는 '22.9월 독일 본에서 열리는 G7 개인정보보호 및 프라이버시 당국 간 '2022 협상 테이블'을 앞두고 공개됐으며, 영국 ICO는 이 자리에서 PET에 대한 작업을 발표하고 PET의 책임 있고 혁신적인 사용 지원을 위한 국제적 합의 주도를 도모
  - 영국 ICO는 PET를 통해 혁신적이고 신뢰할 수 있는 애플리케이션 개발을 촉진하여 조직의 개인정보보호 역량 강화와 함께 민감 정보의 공유와 공동 분석 활동을 확대할 수 있는 제공할 것으로 기대

② 영-미 PET 챌린지 프로그램

▶ 영국은 '22.7월 ICO 주도로 미국 정부와 함께 공동의 사회적 과제 해결의 일환으로 PET의 다양한 가능성을 타진하기 위한 챌린지 프로그램(U.K.-U.S. Prize Challenges)을 착수[6]

6) https://www.whitehouse.gov/ostp/news-updates/2022/07/20/u-s-and-u-k-launch-innovation-prize-challenges-in-privacy-enhancing-technologies-to-tackle-financial-crime-and-public-health-emergencies/

- 양국은 이 챌린지 프로그램 하에서 130만 파운드의 자금을 조성하여 조직이 보유한 개인정보를 공개, 공유, 결합하지 않고 민감 정보에 대한 AI 훈련 모델을 지원할 수 있는 프라이버시 보존형 강화학습 솔루션을 개발키로 함

- 개발 분야는 ▲돈세탁 등 금융 범죄 방지와 ▲프라이버시 보호 하에 개인의 감염 위기를 예방하기 위한 공공 긴급 의료의 2개 트랙으로 진행

- 입상한 솔루션은 '23년 3월 말에 개최될 예정인 '제2차 민주주의 정상 회의(The Second Summit for Democracy)[7]'를 통해 공개키로 함

(2) 미국

▶ **(개요)** 미국 백악관 소속 과학기술정책국(OSTP, Office of Science and Technology Policy)은 '22.6월 프라이버시 강화 기술(PET) 정보 제공요청서(RFI)[8]를 통하여 공공의견 수렴을 실시

- OSTP는 서비스가 부족하거나 소외된 그룹에 대한 형평성을 강화하고 개인정보 처리 및 정보기술(IT)에 대한 신뢰 증진을 포함하여 개인과 사회에 대한 이익을 극대화하는 방식으로 PET의 책임 있는 개발과 채택을 가속화하기 위한 방안을 중심으로 한 달간 의견을 요청

- 의견 요청을 위한 정보제공요청서 작성에는 국가과학기술위원회(NSTC) 산하 네트워킹 및 정보기술연구개발(NITRD) 프로그램의 소위원회인 프라이버시 보존 데이터 공유 및 분석에 관한 신속처리위원회[9]와 국가AI이니셔티브사무국(NAIIO), NITRD 국가조정실이 참여

- 미국 연방정부는 의견 수렴을 통해 개인정보보호 측면에서 데이터 공유 및 분석을 발전시키고 채택하기 위한 국가 전략 개발의 일환으로 개인정보의 안전한 활용 촉진 조치와 권장사항을 검토코자 함
  - 의료, 농업, 행정 등 다양한 분야에서 직면한 문제 해결에 필수적인 자원으로 자리매김한 개인정보의 잠재력을 최대한 발휘하기 위해서는 개인정보보호법, 소비자보호법, 지적재산 관련 법률 등의 분야에서 활용되고 있는 현재의 데이터 모델 훈련과 관련된 제도적 제약을 해소하기 위한 방안 모색

7) 제1차 민주주의 정상 회의는 '21.12월 조 바이든 미국 대통령 주도로 비대면 화상 회의로 진행. 당시 정상회의에서는 약 100개 국가가 권위주의에 대한 방어, 부패와의 싸움, 인권 존중 증진 등 3대 의제, 750개 사항에 대해 약속을 다짐. 제2차 정상회의는 미국, 대한민국, 네덜란드, 잠비아, 코스타리카 공동 주최하며 3월 29일~30일 동안 개최.
https://www.state.gov/summit-for-democracy-2023/
8) Federal Register, Request for Information on Advancing Privacy-Enhancing Technologies, 2022.6.9
9) Fast Track Action Committee on Advancing Privacy-Preserving Data Sharing and Analytics of the Subcommittee

- 특히 OSTP는 연방 차원의 법률, 규정, 부처, 연구 우선순위 및 기타 메커니즘에 관한 의견에 관심을 피력

• PET 분야의 연구, 개발, 조달, 활용 또는 관리 당사자, 연방정부 데이터 교환 전담 직원, PET를 활용한 연방 서비스 제공 경험자 등 제반 이해당사자를 대상으로 의견 청취

▶ **(요청 정보)** OSTP는 ▲연구 기회 ▲기술적 제약 ▲응용 분야 ▲제도/법률 ▲채택에 따른 위기 요인 ▲모범 사례 등을 중심으로 이해당사자들의 의견과 정보를 요청

• **(연구 기회)** 연구, 하드웨어 및 소프트웨어 개발, 교육 및 훈련 프로그램을 포함하여 PET의 개발 또는 채택을 가속화하기 위해 도입 또는 수정할 수 있는 연방 연구 기회에 대한 정보

• **(기술 관련 요청 사항 및 제약)** 특정 유망 PET 기술, 최신 PET 이론 및 실제 적용 사례, 제한된 데이터 및 컴퓨팅 자원으로 인한 제약, 현행 비식별화 및 익명화 기술의 제약 등

• **(응용 분야 및 분석 유형)** PET 채택 가능성이 큰 분야, 애플리케이션 또는 분석 유형에 대한 정보
  - ▲데이터 분산도가 높거나 민감한 분야와 애플리케이션 ▲PET가 일반인에게 중요한 통찰이나 서비스를 제공할 수 있는 분야와 애플리케이션 ▲PET가 의도하지 않은 공개의 위험을 줄일 수 있는 분야와 애플리케이션 ▲PET가 데이터 이동성과 상호운용성을 지원할 수 있는 분야와 애플리케이션 등

• **(제도/법률)** PET 개발 또는 채택을 가속화하기 위해 활용, 개정 또는 신규 도입이 필요한 연방 규정이나 당국에 대한 정보
  - ▲관리예산국(OMB, Office of Management and Budget), 연방거래위원회(FTC, Federal Trade Commission) 및 금융 규제기관 하의 개인정보보호 관련 규칙 제정 기관 ▲기관이 개인정보의 책임 있는 공유를 보장하기 위한 절차를 규정하는 연방 당국 ▲연방 조달 규정(Federal Acquisition Regulation) 등

• **(기타 제도/법률)** 상기 이외의 기타 PET 고도화를 위한 정책 메커니즘
  - 오픈소스 프로토콜과 기술 지침의 개발, 공공-민간 파트너십의 활용, 챌린지 프로그램, 보조금, 테스트베드, 표준, 해외 및 비정부 단체와의 협력, 연방 데이터 전략(Federal Data Strategy) 및 주, 지자체 및 준주 정부와의 개인정보 공유 절차
  - 표준 비공개 계약, 기밀성 조항, 데이터 활용 또는 공유 계약 등의 해석 및 수정

• **(PET 채택 관련 위기)** 위기 완화를 위한 정책, 거버넌스 및 기술 조치뿐만 아니라 PET 채택으로 인한 위기 또는 부정적 결과
  - 서비스를 누리기 어려운 소외 계층에 대한 형평성과 관련된 위기, 채택에 따른 기술 구현의 복잡성 및 자원, PET가 제공하는 기술 보증에 대한 개념적 오해 등을 포함
  - 또한, PET 채택에 따른 위험을 측정하고 사용의 위기-편익 분석을 수행하는 방법에 대한 권고사항도 포함

- **(PET 채택 모범 사례)** 현재 PET 채택 촉진에 도움이 되는 미국 정책 및 책임 있는 채택을 촉진하는 모범 사례에 대한 정보
  - 개인정보보호, 사이버보안, 데이터 분석의 정확성, 서비스 취약 지역에 대한 형평성, 시장 경쟁 등 PET 채택을 지원하는 기존 정책 등

(3) 싱가포르

▶ **(개요)** 싱가포르 정보통신미디어개발청(IMDA)이 '22.7월 개인정보보호위원회(PDPC)와 공동으로 PET 샌드박스 제도를 개시[10)]

- IMDA는 동 샌드박스를 통해 공통의 비즈니스 과제를 해결하기 위한 PET 프로젝트의 시범 운영 기업을 지원할 계획

- 샌드박스에 참여한 조직에 지원하는 서비스는 ▲활용 사례 개발사와 PET 솔루션 공급 리스트 간 매칭 ▲시범 프로젝트의 범위를 지정하고 실행할 수 있도록 활용 사례 개발사에 대한 보조금 지원 ▲규정 준수 하에 PET를 실행할 수 있도록 규제상의 우려를 최소화하기 위한 규제 측면의 지원 등

표2 _ IMDA의 PET 샌드박스 지원 사항

지원 항목	주요 내용
활용 사례 개발사-PET 공급자 간 매칭	◆ 활용 사례 개발사를 대상으로 IMDA가 사전 인증한 제공업체의 솔루션 활용을 지원하여 관련 PET 솔루션 및 제공사 탐색 시간 단축 ◆ 사전 인증 솔루션 제공사는 ▲공통 활용 사례 유형을 해결할 수 있는 관련 PET 솔루션 보유 ▲PET 실행 관련 실적 및 재정적으로 지속 가능한 운영 등 IMDA가 요구하는 기준을 충족해야 함
활용 사례 개발사 보조금 지원	◆ 프로젝트 기간 동안 적격 비용 항목*에 대해 최대 50%까지 보조금 지원 * 적격 비용 항목: 6개월 프로젝트 기간 동안 필요한 인력, 전문 서비스 및 하드웨어/소프트웨어 등
규제 불확실성 해소	◆ 규정 준수 하에 PET를 실행할 수 있도록 규제상의 우려를 최소화하기 위한 규제 측면의 지원 ◆ 프로젝트 전반에 걸쳐 PDPC가 샌드박스에 참여하는 기업에 질문을 해결하고 명확하게 설명하기 위해 규제 지침을 제공

- IMDA는 동 프로그램을 통해 기업들이 데이터 공유 목표를 해결하기 위해 적합한 PET를 확인하고, 기술적 한계에 대한 더 나은 이해를 촉진하는 데 도움이 될 것이라고 언급
  ※ 신청 기간: '22.7.20~'22.10.31

10) IMDA, IMDA and PDPC launch Singapore first Privacy Enhancing Technologies Sandbox as they mark decade-long effort of strengthening public trust, 2022.7.20

▶ **(활용 사례 유형화)** PET 샌드박스는 ▲복수 데이터셋에서의 공통 고객 식별 ▲복수 데이터셋에서의 공통 고객에 대한 추가적인 특징과 속성 추출 ▲AI모델 개발 및 테스트용 데이터의 3대 유형으로 활용 사례를 다음과 같이 구분하여 사업을 지원

- **(복수 데이터셋에서의 공통 고객 식별)** 소매기업 및 보험사가 데이터 공유 파트너십을 체결하기 전에 양사가 공동으로 보유하고 있는 고객의 수를 확인하기 위한 솔루션
- **(복수 데이터셋에서의 공통 고객에 대한 추가적 특징과 속성 추출)** 여행사와 통신사업자가 공동 데이터 모델을 구축하여 상업적으로 민감한 정보를 공개하지 않고 여행 성향을 최적으로 기술하기 위한 기능 구현
- **(AI모델 개발 및 테스트용 데이터)** 투자 기업이 보유한 포트폴리오 기업의 해외 공급망 데이터에 관한 투자 위기관리 AI 모델을 학습시키고자 하나, 규제 또는 기밀성 제약으로 개발에 난항을 겪는 경우

▶ **(제안 PET 솔루션 권고사항)** 활용 사례 개발사는 제안서 제출 시 PET 솔루션 제공 파트너 기업에 대한 제약은 없으며, 필요 시 IMDA가 제시하는 사전 인증 PET 솔루션 개발사 접촉이 가능

- 제안서상의 PET 솔루션은 시장 출시가 가능한 수준으로 개발된 상태이어야 하므로 연구 중심적인 제안서는 본 프로그램에 적합하지 않을 수 있음

▶ **(샌드박스 참가 방법)** IMDA는 싱가포르 등록 기업(활용 사례 개발사)들을 대상으로, 6개월 기간의 프로젝트 제안서를 제출

- PET 샌드박스는 PET 구현 방안 데모와 관련된 활용 사례 중심의 파일럿 프로젝트를 추진 중인 기업들이 참여할 수 있음
- 제안서에는 ▲활용 사례 세부사항과 ▲활용 사례 요구사항을 해결하기 위한 PET 솔루션이 포함되어야 함

▶ **(기대 효과)** 싱가포르 정부는 PET 샌드박스 제도를 통해 개인정보 활용 가치 제고, 산업계 우려 해소 및 민감 정보 보호 등의 효과를 도모

- 암호화를 기반으로 하는 PET는 개인정보 제공자에게 분석용 데이터를 공개할 때 차등 개인정보보호 또는 동형 암호화와 같은 기술을 활용해 원래 형태로는 공개되지 않으며, 연합학습 또는 다자간 컴퓨팅 등의 기술을 통해 공개되지 않은 데이터로부터의 지속적인 분석과 통찰을 제공
- PET의 이 같은 특징은 개인정보 공유에 따른 산업계의 위험 우려를 해소하고, B2B 데이터 협업, 국경 간 개인정보 이동, AI 개발을 위한 다양한 개인정보 활용 촉진에 기여

- 이를 통해 기업은 개인정보 기반 비즈니스 가치 창출과 동시에 개인정보 보호 조치를 강화할 수 있음

• PET를 통해 기업은 개인정보 자체를 노출하지 않고 개인정보에서 필요한 값만 추출함으로써 개인정보와 상업적으로 민감한 정보를 보호할 수 있음
  - PET는 B2B 데이터 협업을 위한 선택의 폭을 넓히고, 국경 간 개인정보 흐름을 가능하게 하며, AI 시스템 개발을 위한 개인정보 가용성을 제고

3. 요약 및 시사점

▶ 본 고를 통해 살펴본 영국, 미국, 싱가포르의 정책 사례는 공통적으로 PET 기술의 시장 정착 촉진과 이에 수반되는 기술 및 제도적 과제를 해결하기 위한 일환으로 추진

표3 _ 주요국 PET 정책 현황 요약

국가	PET 관련 정책	주요 내용
영국	PET 가이던스	◆ PET 도입 촉진을 위해 고려해야 할 법률, 정책, 기술 이슈에 관한 지침 제공
미국	PET 정보제공요청서	◆ 연구 기회 포착과 제도 정착을 위한 공공의견 수렴
싱가포르	PET 샌드박스	◆ 활용 사례 개발사-PET 공급자 간 매칭 활용 사례 개발사 보조금 지원 규제 지침 제시를 통한 PET 활용 시범 사업 지원

• 영국의 PET 가이던스는 PET 도입 촉진을 위해 고려해야 할 법률, 정책, 기술 이슈에 관한 지침을 제공함으로써 규제 측면의 불확실성을 해소하고, 시장 초기 단계에서 기술 적용의 부작용을 완화

• 미국의 PET 정보제공요청서는 연구 기회 포착과 제도 정착의 첫 단계로서 공공의견 수렴을 추진한 사례

• 싱가포르 샌드박스 제도는 PET 활용 사례 발굴 및 확산을 위해 적극적으로 정부가 시장에 개입한 사례로, 공급자 매칭, 보조금 지원, 규제 가이드 등 다양한 분야에 걸쳐 실제적인 사업 지원을 실행

▶ 한편, 우리나라는 개인정보보호위원회가 '22~'26년 5개년 개인정보 기술 R&D 계획을 통해 PET를 ▲유·노출 최소화 ▲안전한 활용 ▲정보주체 권리보장 등 3개 분야로 구분해 로드맵 대상 기술로 선정한 바 있으며, 관련 투자가 뒷받침되고 있음

▶ 그러나 데이터경제 활성화를 위한 PET의 가치 기여를 촉진하기 위해서는, 기술 개발 투자 이외에도, 살펴본 사례와 같이 제도 마련을 위한 이해당사자 간의 포괄적 논의와 상용화로 이어질 수 있는 시범사업 환경 조성 등의 보다 다양한 각도에서의 촉진책 마련을 위한 검토가 필요

Reference

1. Federal Register, Request for Information on Advancing Privacy-Enhancing Technologies, 2022.6.9
2. IMDA, IMDA and PDPC launch Singapore first Privacy Enhancing Technologies Sandbox as they mark decade-long effort of strengthening public trust, 2022.7.20
3. The White House, U.S. and U.K. Launch Innovation Prize Challenges in Privacy-Enhancing Technologies to Tackle Financial Crime and Public Health Emergencies, 2022.7.20
4. UK ICO, ICO publishes guidance on privacy enhancing technologies, 2022.9.7
5. 한국인터넷진흥원, 개인정보보호 강화기술(PET) 동향, 2021

EU 인공지능법(안)과 GDPR의 상호작용 분석

[목 차]

1. 개요

▶ 주요국 개인정보보호 감독기구들은 AI의 도입 속도와 범위가 빠르게 확장됨에 따라 AI 이용과 AI 학습에서의 개인정보의 역할에 대해 관심 증가[11)]

- AI는 프로세스 자동화, 기계학습, 챗봇, 안면인식, 가상현실 등 다양한 분야에서 영향을 미치고 있음
- 개인정보는 조직이 사용하는 AI의 기능에 재료로 활용되기도 하며, 조직은 이를 통해 행동 경향을 파악하며 향후 결과를 예측

11) CSO, European data protection authorities issue record €2.92 billion in GDPR fines, 2023.1.17

- 많은 AI 시스템이 개인정보를 사용하기 때문에 AI 시스템 규제는 종종 GDPR의 규제 범위에 속하며, 개인정보보호 감독기구들도 AI 환경에서의 개인정보보호를 검토

▶ 2021년 이후 EU는 인공지능법(AI Act) 제정을 추진 중이며, 제안된 인공지능법안[12]은 EU 일반개인정보보호법(이하 GDPR)과 상호작용 관계를 형성

- 개인정보보호 관련 기본적 권리는 AI 시스템의 전체 수명 주기 동안 보장되어야 함
- 개인정보 처리가 개인의 기본권에 중대한 위험을 수반할 때 개인정보 처리자는 EU GDPR에 따라 '개인정보 최소화 원칙', '설계 및 기본설정에 의한 개인정보보호 원칙'을 필수로 준수해야 함
- AI 시스템 제공자와 사용자는 개인정보보호 권리를 보장하기 위해 기술적·관리적 조치를 구현해야 함

▶ GDPR은 제22조*에서 개인정보를 처리하는 AI 기술에 대한 의무를 일부 규정하고 있지만, 인공지능법은 GDPR 제22조 조항보다 훨씬 명료하고 광범위한 요건을 규정

* GDPR 제22조: 프로파일링 등 자동화된 개별 의사결정(Article 22 GDPR. Automated individual decision-making, including profiling)

▶ 2022년 12월 유럽개인정보보호기구연합(CEDPO)*은 AI 시스템의 개인정보 활용이 증가하는 상황 하에 GDPR 시행과 인공지능법 제정 추진 등 새로운 법률 환경에서 인공지능법이 개인정보보호관리자(DPO)**의 역할에 미치는 영향에 관한 의견서*** 발표

* Confederation of European Data Protection Organisations: 개인정보보호 책임자의 역할 촉진, 균형 있고 실행 가능하며 효과적인 개인정보보호 조언, EU 개인정보보호 관련 법률의 관행을 개선하는 역할 수행

** Data Protection Officer

*** CEDPO Opinion on the potential impact of the EU's proposed Artificial Intelligence Act (AI Act) on the role of the data protection officer(2022.12.20.)

▶ 본 고에서는 CEDPO의 의견서를 기반으로 인공지능법(안)과 GDPR의 상호작용이 가지는 중요성, 상호작용 영역을 비롯해 특히 인공지능법(안)으로 인한 새로운 법률 환경이 개인정보보호관리자의 역할에 미치는 영향을 고찰하고자 함

12) European Commission, Artificial Intelligence Act, 2021.

2. 인공지능법(안) 및 GDPR에서 주요 역할 연관성

(1) 인공지능법(안)과 GDPR의 책임과 역할의 중복

▶ GDPR에 정의된 개인정보 처리자로서의 컨트롤러, 프로세서 및 공동 컨트롤러의 기존 책임이 인공지능법(안)에 정의된 주요 역할(제공자, 사용자, 수입자, 유통자)에 어떻게 매칭이 되는지 명확한 이해 필요

▶ 인공지능법(안)에 데이터(개인정보 또는 非개인정보)와 AI 시스템 사이의 강한 연관성이 반영되어 있음

- 개인정보보호, 프라이버시 보호, 통신기밀 보안에 관한 EU의 법률들은 인공지능법(안)이 규정하는 권리·의무와 관련된 개인정보 처리에 적용됨
  ※ 그러나 인공지능법(안)은 EU의 GDPR 규정에 영향을 미치지 않음

▶ GDPR-인공지능법(안) 사이에 발생하는 상호작용에 중요한 특징으로 각각의 법률을 준수하도록 요구되는 다양한 플레이어(Player)들의 책임과 의무에서 중복이 발견됨

- GDPR에서의 컨트롤러, 프로세서, 공동 컨트롤러와 인공지능법(안)에서의 제공자, 사용자, 수입자, 유통자 간 의무와 책임에서 중복 발생 가능
- 인공지능은 일반적으로 여러 단계나 목적을 위해 개인정보를 처리하므로 하나의 특정 제공자, 사용자, 수입자, 유통자가 일부 단계나 목적을 위해서는 컨트롤러 또는 공동 컨트롤러 역할을 담당하고, 다른 단계나 목적을 위해서는 프로세서의 역할 가능
- 인공지능법(안)에서 대부분의 의무사항은 제공자를 적용 대상으로 하고 있으나, 일부 의무사항은 사용자, 수입자, 유통자를 적용 대상으로 함

▶ 제공자 관련, 인공지능법(안)은 고위험 AI 시스템의 설계 및 개발부터 시장 출시나 서비스 배포 전, 또는 그 이상 AI 시스템의 전체 수명 주기에서 준수해야 하는 필수 요건들을 규정, 이러한 요건 중 일부는 개인정보 처리와 관련되어 GDPR의 적용을 동시에 받을 수 있음

(2) 인공지능법(안)과 GDPR의 중복 및 중첩 분야

▶ **(위험관리체계)** 인공지능법(안)에 따라 제공자가 수행하는 위험 평가는 GDPR의 제24조, 제25조, 제32조 및 제35조에 따라 컨트롤러로서 제공자나 사용자가 수행해야 하는 위험 분석과 중복 및 중첩될 수 있음

※ GDPR 제24조: 컨트롤러의 책임
※ GDPR 제25조: 설계 및 기본설정에 의한 개인정보보호
※ GDPR 제32조: 처리의 보안
※ GDPR 제35조: 개인정보보호 영향평가

- 인공지능법(안)에 따라 제공자는 인공지능법(안) 준수를 보장하는 체계를 문서로 구현하고 고위험 AI 시스템이 개인의 기본권에 미칠 수 있는 널리 알려진 위험과 합리적으로 예측할 수 있는 위험을 식별·분석하고, 위험 수준을 평가하고, 적절한 조치를 수행해야 함

▶ **(데이터 거버넌스)** 인공지능법(안)에 따라 고위험 AI 시스템을 개발하고 사용할 때 해당 시스템의 전체 수명주기에서 GDPR의 제5조제(1)항제(c)호 및 제25조에 각각 언급된 '개인정보 최소화', '설계 및 기본설정에 의한 개인정보보호'의 원칙을 적용해야 함

- 인공지능법(안) 제10조(데이터 및 데이터 거버넌스)는 유해 및 차별적 편견을 줄이기 위해 제공자가 학습, 검증 및 시험에 사용하는 데이터에 대해 데이터 거버넌스 표준을 준수하고, 관련성, 대표성, 정확성, 완전성과 관련해 높은 수준의 요건을 규정

※ GDPR 제5조: 개인정보 처리 원칙
※ GDPR 제5조제(1)항제(c)호: 처리되는 목적과 관련하여 적절하고, 타당하며, 필요한 정도로만 제한('개인정보 최소화')

▶ **(로그 유지)** 인공지능법(안)에 따라 고위험 AI 시스템의 의도된 목적과 EU 또는 자국법에 따른 법적 의무에 따른 기간 동안 로그를 보관해야 하며, 컨트롤러의 저장기간 제한 원칙 준수에 관한 GDPR의 제5조(1)(e)에 의거 로그를 보존해야 함

- 인공지능법(안) 제12조(기록 유지)는 제공자가 고위험 AI 시스템이 통제 범위 내 있다고 가정하고 고위험 AI 시스템의 결정과 프로세스에 대한 검증 및 추적 가능성을 보장하도록 규정

- 자동 로그 기록 메커니즘 제공, 오작동·오용 사후 감사, 전체 수명 주기 동안 시스템의 적절한 기능 보장, 모니터링 등을 통해 검증·추적 가능

※ GDPR 제5조제(1)항제(e)호: 처리목적 달성에 필요한 기간만 정보주체를 식별할 수 있는 형태로 보관. 개인정보는 제89조제(1)항에 따라 정보주체의 권리 및 자유를 보호하기 위해 본 규정이 요구하는 적절한 기술·관리적 조치를 시행하여 공익적 기록 보존, 과학· 역사적 연구, 통계 목적을 위해 처리되는 경우 더 오랜 기간 보관 가능

▶ **(위임대리인 지정)** 인공지능법(안)의 제25조(위임대리인)의 위임대리인에 관한 규정은 GDPR 제3조제(2)항에서 명시한 영역에 따른 컨트롤러와 프로세서의 의무와 관계될 수 있음

- 인공지능법(안) 제25조는 EU 역외에 소재한 제공자는 EU 시장에서 AI 시스템을 사용하기 전에 서면 위임으로 EU 역내에서 설립한 위임대리자를 지정하도록 규정

- GDPR 제3조제(2)항은 GDPR의 적용 영역을 정의하면서 EU 역외에 소재한 컨트롤러 또는 프로세서가 EU 역내에 거주하는 정보주체의 개인정보를 처리할 때도 적용되도록 규정

▶ **(이외 사항)** 인공지능법(안) 규정들은 GDPR에서 일반적으로 컨트롤러나 프로세서에 부과된 의무사항들을 사용자들에게 추가

- **(처리 담당자 지정)** 인공지능법(안) 제14조(인간의 감독)에 따라, 고위험 AI 시스템의 사용자는 고위험 AI 시스템에 대한 인간 감독자가 유능하고 적절한 자격을 갖추고 교육을 수료하고, 효과적인 감독을 위해 필요한 자원을 확보하도록 보장해야 함

- **(개인정보 관련성)** 사용자는 공정성, 목적 제한, 최소화 및 정확성에 대한 GDPR의 원칙을 반영하여 고위험 AI 시스템의 의도된 목적을 고려하여 개인정보와의 관련성을 확인해야 함

- **(개인정보보호 영향평가)** 해당되는 경우, 고위험 AI 시스템 사용자는 시스템의 기술적 특성, 용도 및 AI 시스템의 상황을 고려하여 GDPR에 따라 개인정보보호 영향평가를 수행해야 함

- 개인 관련 결정이나 결정을 지원하는 고위험 AI 시스템 사용자는 고위험 AI 시스템이 이용한다는 사실을 개인에게 알려야 함

3. 인공지능법(안) 및 GDPR에서 위험 평가

▶ 인공지능법(안)과 GDPR에 의무사항에서 주요한 중첩은 개인정보 처리와 AI 시스템의 융합으로 인한 개인에 대한 위험 관리에서 집중적으로 발생

- GDPR는 설계 및 기본설정에 의한 개인정보보호 원칙 및 개인정보보호 영향평가 수행을 통해서 개인정보 처리와 AI 시스템의 융합에 따른 개인에 대한 위험 관리

- 반면, 인공지능법(안)은 적합성 평가 및 위험 관리를 수행하며, 가능한 경우 개인정보보호 영향평가 수행

▶ AI 시스템에 대한 우려는 AI 시스템이 정보주체에 직·간접적인 영향을 끼치는 다음과 같은 경우에 발생

- AI 시스템이 정보주체에 직접적인 영향을 미치는 개인정보 처리의 경우(예: 안면 인식, 신용 평가, 출입국 심사)

- AI 시스템의 개인정보 처리가 정보주체와 상호작용을 하는 환경에 영향을 미치는 경우(예: 자율주행 시스템, 의료 진단 시스템)

▶ GDPR은 자동화된 의사결정 또는 프로파일링을 수행하는 AI 시스템에 대해 개인정보보호 영향평가를 수행하도록 규정

- GDPR에 의거, 이용 중인 대다수의 AI 시스템, 특히 개인(Natural Persons)에게 영향을 미치는 모든 AI 시스템이 개인정보보호 영향평가의 적용 대상일 수 있음

- AI 시스템이 자동화된 의사결정 또는 프로파일링의 기준을 완벽히 충족하지 않을 때에도 개인정보 데이터셋을 매칭 혹은 결합하거나 AI 관련 신기술을 적용하면 유럽개인정보보호이사회(EDPB*)의 '개인정보보호 영향평가 지침**'에 따라 개인정보보호 영향평가 필요

* European Data Protection Board

** Guidelines on Data Protection Impact Assessment

▶ 반면 인공지능법(안)은 제29조제(6)항에서 개인정보보호 영향평가에 관한 요건을 '해당되는 경우(where applicable)'로 제한하고 있으나, 실제적으로는 다수의 AI 사용 사례가 개인정보보호 영향평가의 적용 대상일 수 있음

※ 인공지능법(안) 제29조: 고위험 AI 시스템 사용자의 의무

※ 인공지능법(안) 제29조제(6)항: 고위험 AI 시스템 사용자는 GDPR의 제35조에 따라 개인정보보호 영향평가를 수행할 의무를 준수하기 위해 제13조에 제공된 정보를 사용(해당되는 경우)

▶ 인공지능법(안)에 의거, 개인정보보호 영향평가의 적용 대상이 증가함에 따라 개인정보보호 영향평가를 자문하는 사람들(대부분 DPO)이 해야 할 일이 평소 업무보다 상당히 증가할 전망

- 인공지능법(안) 제29조제(6)항은 고위험 AI 시스템 사용자에게 개인정보보호 영향평가 의무를 준수하기 위해 제13조에 의거해 제공된 정보를 사용하도록 규정

- 반면, GDPR은 AI 시스템 공급자가 개인정보보호 영향평가 관련 정보 제공 의무를 규정하지 않으며, 이러한 불균형은 개인정보보호관리자에 부담으로 작용

- 개인정보보호 영향평가 방식의 위험 분석이 AI 시스템 위험 관리에 관한 인공지능법(안)의 의무를 충족하는지 여부는 아직은 명확히 판단할 수 없으며, 아직 명확한 지침이 없는 상황에서 불필요한 노력의 중복이 발생할 가능성이 있음

- 사용자이자 동시에 공급자인 경우 인공지능법(안)의 제3장(고위험 AI 시스템의 사용자 및 기타 당사자의 의무사항)에 따른 의무사항이 개인정보보호관리자에 부과될 수 있음

표 _ 인공지능법(안)의 제3장(제16조~제29조)

조항	내용	조항	내용
제16조	고위험 AI 시스템 제공자의 의무	제23조	당국과 협력
제17조	품질관리시스템	제24조	제품제조자의 의무
제18조	기술문서 작성 의무	제25조	위임대리인
제19조	적합성 평가	제26조	수입자 의무
제20조	자동 생성 로그	제27조	유통자 의무
제21조	시정 조치	제28조	유통자, 수입자, 사용자 또는 기타 제3자의 의무
제22조	정보 의무	제29조	고위험 AI 시스템 이용자의 의무

4. 인공지능법(안)이 개인정보보호관리자(DPO)에 미치는 영향

▶ 개인정보와 AI 시스템 간 중첩이 발생하는 상황에서 DPO 역할에 대한 우려

- DPO가 AI 소프트웨어 관련 기술적 고려사항에 능숙해지려면 DPO의 법적 독립성이 손상되거나 DPO의 전문성을 넘어선 문제에 직면할 수 있음
- 조직 내 DPO의 역할은 엄격한 개인정보보호 법률 지침에 따라 GDPR 및 기타 관련 EU 또는 회원국이 개인정보보호 규정을 준수하도록 조언하는 데 중점을 맞출 필요가 있음

▶ 인공지능법(안)에서 DPO의 역할에 대한 명확화 필요

- GDPR에서 DPO의 역할은 제37조(DPO 지정), 제38조(DPO 지위), 제39조(DPO 임무)에 명확히 근거하고 있으나, 인공지능법(안)은 개인정보보호 법률 준수 및 규제를 감독하는 역할(역할 담당자)을 명확히 규정하지 않음
- GDPR의 DPO의 역할 정의와 마찬가지로 인공지능법(안)도 DPO 역할을 명확히 규정할 필요

▶ 예측 가능한 위험 감소를 위해 DPO 역할에 대한 명확화가 필요

- DPO가 조직 내에서 AI 활동에 대한 책임을 맡는 경우(예: AI 시스템 실행 기능, AI 시스템 처리 활동 정의), 이는 DPO의 역할 독립성 침해와 GDPR 제38조제(6)항이 규율하는 이해 상충을 초래하는 업무 및 직무를 DPO에게 할당하지 못하도록 한 규정을 위반하게 될 수 있음

※ GDPR 제38조제(6)항: DPO는 기타 업무 및 직무를 수행할 수 있으며, 컨트롤러나 프로세서는 이러한 업무 및 직무가 이해의 상충을 초래하지 않도록 해야 함

※ 벨기에 개인정보 감독기구는 2020년 4월 GDPR 제38조제(6)항의 이해의 충돌 금지 규정을 위반한 사항에 대해 컨트롤러에 50,000유로 과징금 부과[13)]

※ 베를린 개인정보 감독기구는 2022년 9월 GDPR 제38조제(6)항의 이해의 충돌 금지 규정을 위반한 사항에 대해 컨트롤러에 525,000유로 과징금 부과[14)]

13) EDPO, DPO and conflict of interest: the Belgian DPA issues a 50,000 EUR fine, 2020.4
14) DataGuidance, Berlin: Berlin Commissioner fines retail group subsidiary €525,000 for DPO conflict of interest, 2022.9

▶ DPO가 GDPR의 규정 관리와 동시에 AI 규정 관리를 책임지는 것은 적절하지 않을 수 있음

- 그러나, DPO가 개인정보만 관련되는 인공지능법(안) 조항을 관리하고 이외 부분은 AI 관리자가 책임지기도 어려울 수 있으며, 두 책임자가 하나의 법률을 준수하기 위해 작업하는 것은 혼란, 갈등 및 반복의 원인이 될 수 있음

▶ 인공지능법(안)이 AI 알고리즘을 사용하여 기존 데이터에서 개인을 식별할 수 있도록 하는 파생(Derived) 개인정보의 생성과 이용을 통제하는 경우 인공지능법 제정이 DPO에 긍정적인 결과를 유발할 수 있음

- AI를 사용하여 CCTV 이미지 또는 GPS 위치 데이터를 분석하여 과거 위치정보 또는 개인의 성적 취향과 같은 개인정보를 식별할 수 있음

- AI 처리 제공자나 사용자에게 파생 개인정보를 명확하게 식별하고 분류하도록 규정하면 개인정보 처리 활동에 대한 정확한 최신 기록을 유지해야 하는 DPO의 직무에 도움이 될 수 있음

5. AI 규제 기관과 개인정보보호 규제 기관의 상호작용

▶ 인공지능법(안)에 따라 기존 규제 기관 외에 회원국에서 독립적인 AI 규제 기관을 설립하는 경우 개인정보보호 규제 기관과 AI 규제 기관의 이해관계에 대한 조사, 집행, 자국 규제 기관과 EU 기관과 상호작용 등이 이슈로 대두될 수 있음

▶ 유럽 개인정보보호감독관(European Data Protection Supervisor, EDPS)은 인공지능법(안)의 적용 범위에 속하는 EU 기관, 단체 등에 행정 과징금을 부과할 수 있으나, 다른 규제 기관과의 관계 설정은 명확하지 않음

- GDPR에 대한 EDPB와 상응하는 AI 관련 규제 기관으로 유럽인공지능위원회(European Artificial Intelligence Board, EAIB)가 있으나 동 기관은 집행 권한이 없음

- 유럽인공지능위원회의 과징금은 GDPR에 따른 과징금보다 훨씬 클 수 있지만 유럽인공지능위원회는 집행 권한이 없으며, 인공지능법(안)은 과징금을 집행할 책임자를 직접 지정하지 않으며 규정을 이행하기 위한 규칙과 법률 제정은 모든 회원국에게 위임

- 인공지능법(안)에 따른 감독과 규정 준수는 회원국에 맡겨져 있어 회원국 간 법의 관리와 적용 측면에서 상당한 차이가 발생할 수 있음

6. 인공지능법(안) 및 GDPR에서의 정보주체 권리 보호

▶ GDPR에 의해 확립된 정보주체의 권리 기반 조치 활동은 인공지능법이 적절히 작동하는지에 따라 달라질 수 있으며, 특히 개인정보보호와 AI 모두와 관련된 사안에서는 이중 규제 장치로 작동할 수 있음

- GDPR은 명확하게 권리 기반의 법안이지만 인공지능법(안)은 권리 기반이라고 명시하지 않으며, 향후 두 개의 법률이 필연적으로 연관될 가능성이 있지만 GDPR에 따라 시작된 권리들이 인공지능법(안)과 상호작용하면서 어떻게 조정될 것인지 명확하지 않음

▶ GDPR에서 민원 처리는 중요하며 일부 감독기구가 개인정보보호 민원을 해결하는 데 수년이 소요되고 있는 상황에서 인공지능법 제정이 민원 처리 프로세스에 미치는 영향 분석이 필요

- 개인정보와 AI와 관련된 민원 처리에서 정보주체가 별도의 규제 기관에 각각 민원 사항을 제출하는 경우 이미 복잡하고 느린 분쟁 해결 프로세스가 더욱 길어질 우려가 있으며, 정보주체가 사법 판결을 얻기가 더욱 어려워질 수 있음

▶ 민원을 처리할 수 있는 역량을 확립하기 위한 기준 고려 필요

- 민원의 불만 사항이 기술적 문제를 포함하는 경우 AI 규제 기관이 더 적절하게 조사할 수 있고, 개인정보보호 규제 기관은 민원 처리에 어려움을 겪을 수 있음
- 반대로, 민원 사항이 개인정보보호법의 문제와 밀접한 경우 전문적 지식을 보유한 개인정보보호 규제 기관이 처리할 수 있으나, 이러한 문제를 다룰 적절한 AI 규제 기관이 없을 수 있음

▶ 다양한 규제 기관이 권리에 대한 다각도의 접근 방식을 취할 위험이 있음

- 동일한 주제에 대해 유럽개인정보보호이사회(EDPB)와 유럽인공지능위원회(EAIB)가 다른 접근 방식의 지침을 내릴 수 있음
- AI 규제 기관은 개인정보보호 외에도 다른 우선순위가 높은 사항을 다룰 수 있지만, 개인정보보호 규제 기관은 특정한 하나의 우선순위, 즉 개인정보보호에만 집중

▶ 인공지능법(안)은 개인에 대한 위험을 해결하려고 하지만 GDPR은 개인의 권리를 보호하는 방법에 중점을 둘 수 있음

7. 결론 및 시사점

▶ AI 시스템에서 개인정보의 활용이 증가하고, 이로 인한 개인정보 침해 우려가 증가함에 따라, 개인정보보호 관리자가 EU의 인공지능법 등 새로운 법률 환경에서 적절한 기술적·관리적 개인정보보호 조치를 준비할 수 있도록 지침 제공 필요

▶ GDPR과 인공지능법(안) 사이에 새로운 종속성이 생성될 법률적 회색 지대를 탐구하고 개인정보보호 규제, 기업의 개인정보보호, AI 기술에 대한 개인정보보호 연구개발 등 다양한 측면에서 정책 입안자들의 검토 필요

▶ EU 및 미국 등 주요국들의 인공지능법 제정 추진에 대한 동향을 지속적으로 분석하고, 국내 개인정보보호 관련 규제 검토 및 개선방안 도출 필요

Reference

1. CEDPO, CEDPO Opinion on the potential impact of the EU's proposed Artificial Intelligence Act (AI Act) on the role of the data protection officer, 2022.12.19.
2. CSO, European data protection authorities issue record €2.92 billion in GDPR fines, 2023.1.17.
3. European Commission, Artificial Intelligence Act, 2021.
4. European Commission, General Data Protection Regulation(GDPR), 2016

해외 아동 개인정보 침해 관련 행정처분 사례 분석
- 미국과 스페인 사례를 중심으로 -

[목 차]

1. 개요

▶ **(배경)** 코로나19 대유행 기간을 거치면서 최근 청소년의 인터넷 이용시간이 대폭 증가한 것으로 조사되면서 미성년자의 개인정보 침해 가능성 증가가 점차 대두

- 한국언론진흥재단의 조사 결과('22년 11월)에 따르면 10대 청소년(초등학교 4학년~고등학교 3학년 학생)의 인터넷 이용시간이 '19년 하루 4시간 반에서 '22년 하루 8시간으로 급격히 증가한 것으로 나타남

- 청소년이 주로 활용한 인터넷 서비스 형태는 온라인 동영상 플랫폼, 인터넷 포털, 메신저 서비스 등으로 다양했고, 게임 플랫폼, OTT서비스, 소셜미디어 서비스, 음악 스트리밍 서비스 등도 많이 이용된 것으로 조사

- 미성년자의 온라인 활동이 늘어날수록, 이들이 성인에 비해 상대적으로 위험에 대한 인식이 낮고 경험이 부족하다는 점을 악용해 미성년자에 대한 개인정보 침해 시도도 증가할 수밖에 없음

▶ **(아동 등 개인정보보호 지원)** 이러한 상황에서 미성년자의 개인정보 침해 위험을 최소화하고자 개인정보보호위원회는 '22년 7월 아동·청소년의 안전한 온라인 활동을 지원하기 위해 「아동·청소년 개인정보 보호 가이드라인」을 마련

- 동 지침에서는 인터넷 환경에서 아동·청소년의 개인정보를 처리하는 사업자 등이 준수해야 하는 사항에 대해 개인정보 처리단계별 행동요령을 제시한 바 있음

▶ **(취지)** 이와 같은 배경을 토대로 아래에서는 '22년 하반기 주요국에서 발생한 미성년자 개인정보 침해 관련 주요 제재 사례를 분석하고자 함

- 주요 사례의 사실관계 및 법적 쟁점을 분석함으로써 해당 연령대 이용자의 개인정보를 취급하는 개인정보처리자에 아동·청소년 개인정보보호 조치에 관한 다양한 통찰력을 제공하고자 하는 취지

2. 미국 연방거래위원회의 에픽게임즈 제재 사례

(1) 서론

▶ 미국 연방거래위원회(Federal Trade Commission, 이하 FTC)는 온라인 슈팅 게임 포트나이트(Fortnite)의 제작사인 에픽게임즈(Epic Games, Inc.)에 총 5억 2,000만 달러를 납부하도록 하는 제재 부과에 합의('22.12.19.)

- 에픽게임즈는 느슨한 개인정보보호 정책을 통해 미성년자를 유해한 환경에 방치했으며, 다크 패턴[15]을 사용함으로써 이용자가 의도치 않은 지출을 하게 한 것으로 드러남

- 이번 사례에서는 주로 ▲온라인상에서의 미성년자 개인정보 침해 조장 및 방치 ▲다크 패턴 활용에 따른 온라인 사업자의 불공정행위 등이 쟁점이 됨

(2) 사실관계

▶ **(개요)** 포트나이트는 전 세계적으로 4억 명이 넘는 이용자를 보유하고 있는 인기 온라인 게임으로, 무료 다운로드를 통해 게임을 즐길 수 있지만 게임 내 의상과 같은 앱 내 아이템에 대해서는 이용자에게 요금을 부과하는 부분 유료 게임 서비스

15) 이용자를 고의적으로 속여 이익을 얻기 위해 설계된 온라인상의 사용자 인터페이스를 의미

- 포트나이트는 세이브 더 월드(Save the World), 배틀로얄(Battle Royale), 포크리(Fortnite Creative) 등 세 가지 모드의 서비스를 지원
- 그중 배틀로얄 모드는 최대 99명의 게임 플레이어와 매칭이 이루어진 후 음성 및 채팅을 통해 상대방과 의사소통하며 게임을 전개하는 형식

▶ **(문제점)** 에픽게임즈는 성인과 미성년자가 같이 게임을 즐긴다는 사실을 알고 있었음에도 불특정 성인이 어린이 및 청소년과 대화할 수 있도록 게임을 설계했으며, 화면 구성에서는 다크 패턴을 활용하여 의도하지 않은 부당한 결제를 유도

- 에픽게임즈는 포트나이트 게임 내 대화 기능(음성 및 채팅을 모두 포함)의 기본값을 연령을 구분하지 않고 모두 활성화로 설정
- 또한 13세 미만의 이용자로부터 개인정보를 수집하면서 부모에게 통지하거나 동의를 얻지 않음
- 한편, 사용자 인터페이스를 악의적으로 조정하여 이용자로 하여금 원치 않는 앱 내 구매를 유도하기도 함

▶ 이와 관련, '17년 초 에픽게임즈 직원들은 어린이들에게 미치는 부정적 영향을 우려하여 아동 계정의 기본설정을 변경할 것을 회사에 제안했으나 회사는 소극적인 대응 방식을 견지

- 에픽게임즈는 포트나이트 이용자인 아동이 성희롱 등 괴롭힘 피해를 입었다는 사실을 인지하였음에도 불구하고 기본설정을 변경하지 않았음
- 이후 이용자에게 음성 채팅을 끌 수 있는 버튼을 추가하는 등 피해의 최소화를 위해 노력했으나 이용자가 해당 버튼을 찾기 어렵도록 설계

(3) 쟁점 판단

▶ **(아동 온라인 개인정보보호법 위반)** FTC는 에픽게임즈의 일련의 행위에 대해 다음과 같이 아동 온라인 개인정보보호법(Children's Online Privacy Protection Act, 이하 COPPA) 위반이라고 판단

- **(동의 흠결)** 에픽게임즈는 상당수의 미성년 이용자가 게임을 즐기고 있다는 사실을 파악하고 있음에도 부모로부터 동의를 얻지 않고 미성년자의 개인정보를 수집
  - 게임사에 자녀의 개인정보 삭제를 요청한 부모에게는 무리한 절차를 요구하거나 삭제 요청을 거부

- **(유해한 기본설정)** 게임의 기본설정이 음성 대화 및 채팅 활성화 상태로 되어 있어, 미성년자가 낯선 성인 이용자와 함께 플레이하는 것을 방치함으로써 미성년 이용자를 위험에 빠뜨림

  - 실제로 어린이 및 청소년 이용자는 온라인상에서 괴롭힘을 당하거나 위협을 받았으며, 자살 등 유해한 이슈에 노출되었음

▶ **(연방거래위원회법 위반)** FTC는 또한 에픽게임즈의 다크 패턴 악용행위 등과 관련, 연방거래위원회법(Federal Trade Commission Act)이 금지하고 있는 불공정행위를 저지른 것으로 판단

- **(다크 패턴 활용)** 에픽게임즈는 전체 이용자로 하여금 의도하지 않은 앱 내 구매를 유발케 하는 것을 목적으로 다양한 유형의 다크 패턴을 사용

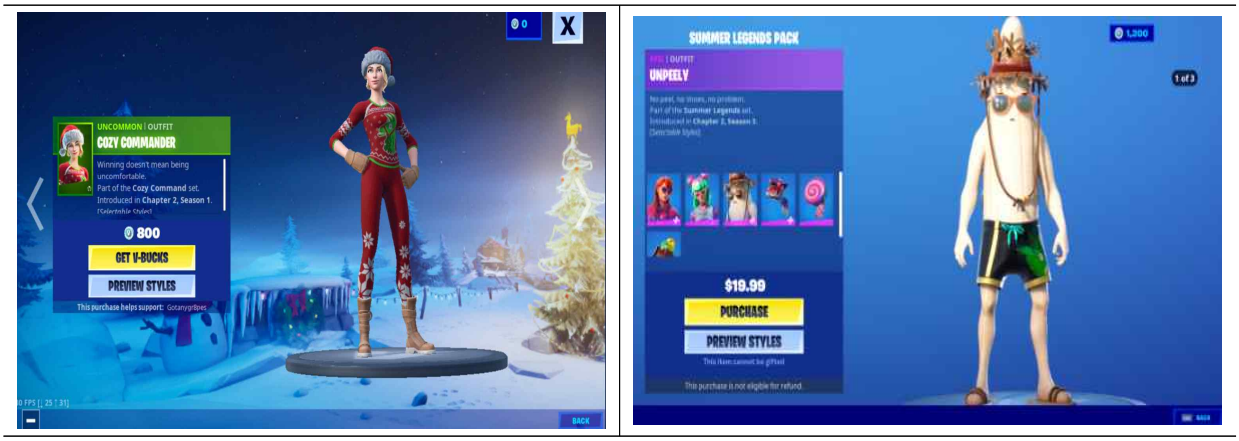
  - 이 사안에서 문제된 것은 포트나이트 게임 내 구성 및 디자인상의 문제로 인해 이용자가 단순한 버튼 클릭만으로 원치 않는 요금이 부과되는 사례가 빈번히 발생한 것으로,

  - 구체적으로는 게임 내에서 단순히 항목 미리보기를 시도하려고 할 때 화면 구성상 인접한 버튼을 클릭함으로써 의도하지 않은 결제가 발생할 수 있었다는 점임

  - 예를 들어, 아래와 같이 게임 내 의상을 구매하기 전 '미리보기'하는 버튼이 '구매' 버튼 바로 아래에 위치

  - 이 때 이용자가 인접한 버튼인 '구매' 버튼을 클릭할 경우 이용자의 게임 내 화폐인 브이벅스(V-Bucks) 잔액에서 해당 항목의 비용을 즉시 공제

그림1 _ 포트나이트 게임 내 버튼 배치 예시



출처 : 포트나이트 아이템샵 트위터('19.12.)[16], Kotaku 뉴스 기사('20.7.)[17]

16) https://twitter.com/itemshopnews/status/1209625780260487168
17) https://www.kotaku.com.au/2020/07/oh-god-fortnite-made-peely-worse/

- **(승인되지 않은 요금 청구)** 이용자는 앱 내에서 미리 구매한 브이벅스를 이용하여 콘텐츠를 구매할 수 있는데, 에픽게임즈는 아동 이용자가 어떠한 인증 절차 없이 신용카드를 이용하여 브이벅스를 구매할 수 있도록 허용

  - 아동 이용자는 부모나 카드소유자의 동의 없이, 구체적으로 신용카드 비밀번호 또는 CVV번호 입력 없이 버튼을 누르기만 하면 계정에 연동된 신용카드를 통해 브이벅스를 구매할 수 있었음

  - 심지어 일부 부모는 자녀의 행위로 인해 에픽게임즈로부터 수백 달러의 신용카드 요금을 청구받기도 함

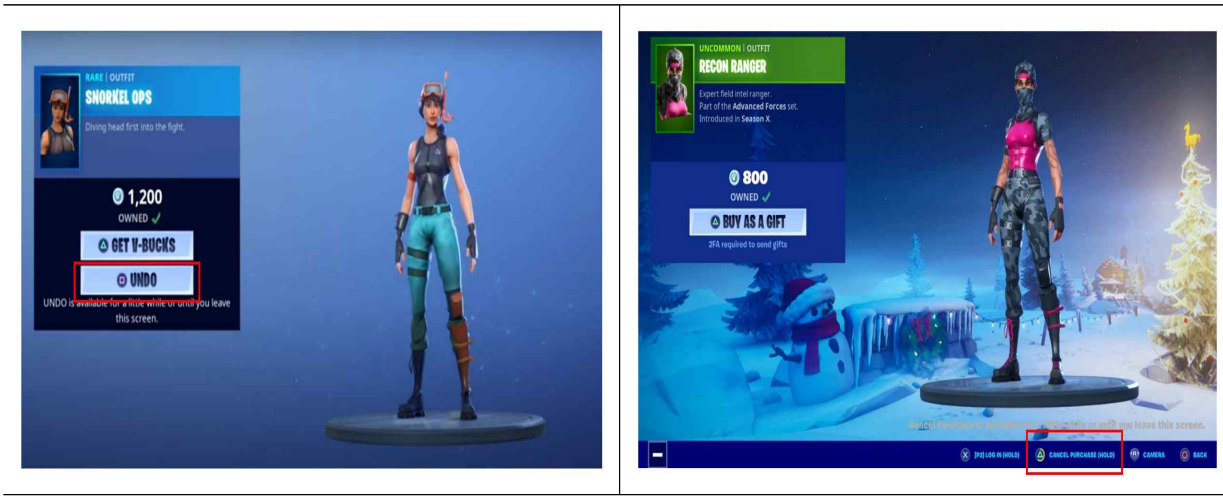
- **(계정 차단)** 에픽게임즈는 부당한 신용카드 대금청구를 근거로 민원을 제기한 고객의 계정을 일시적으로 차단

  - 계정이 차단된 이용자 입장에서는 앱 내에서 구매했던 아이템, 스킨 등 모든 콘텐츠에 대한 접근 권한을 상실하는 것으로 이는 수천 달러의 피해와 상응하다고 볼 수 있음

  - 이용자가 계정 차단을 해제해 줄 것을 요청하는 경우 향후 요금과 관련한 이의를 제기할 시 계정이 영구 차단될 수 있음을 경고하기도 함

  - 이 과정에서 에픽게임즈는 내부 테스트를 통해 취소 및 환불 버튼을 의도적으로 눈에 띄지 않게 재배치하는 등 취소 및 환불을 더욱 어렵게 한 것으로 드러남

그림2 _ 포트나이트 게임 내 취소 및 환불 버튼 재구성 예시[18)]



출처 : FTC 심판개시결정문(Complaint) ('22.12.)

18) 붉은 색 네모 처리한 결제취소 버튼이 기존에는 화면 중앙에 크게 배치되어 있었으나(왼쪽 그림), 이후 화면 우측 하단으로 작게 디자인되어 이동(오른쪽 그림)한 것을 확인할 수 있음

(4) 제재

▶ FTC는 법적 절차를 중단하고 에픽게임즈와 동의명령합의(consent agreement)[19]를 체결하여 사안을 종결하기로 합의

- 양측이 체결한 동의명령합의는 각각 ▲아동 개인정보 침해 ▲불공정행위와 관련한 별개의 두 건의 합의문으로 구성

위반법률·조항	제재 내용
아동 온라인 개인정보보호법 제1303조	• **(금전적 제재)** 에픽게임즈는 아동 온라인 개인정보보호법(COPPA) 위반에 대해 2억 7,500만 달러의 민사 제재금을 납부할 것 • **(개인정보 삭제 조치)** 부모에 대한 통지 및 동의 요건을 위반하여 게임 이용자로부터 수집한 개인정보를 모두 삭제할 것 • **(개인정보보호 정책 변경 조치)** 아동 및 청소년 이용자의 음성 및 채팅 대화 기능은 비활성화로 변경 설정하는 등 강력한 개인정보보호 정책을 채택할 것
연방거래위원회법 제5조	• **(금전적 제재)** 에픽게임즈는 다크 패턴 및 이를 기반으로 소비자를 기만하여 의도하지 않은 결제를 유도한 행위에 대해 2억 4,500만 달러의 행정 제재금을 납부할 것 (이 금액은 소비자에게 환불될 예정) • **(부당한 비용청구 금지)** 다크 패턴을 악용하여 이용자에게 비용을 청구하거나 명확한 승인 절차 없이 이용자에게 요금을 청구하지 않을 것 • **(부당한 계정 차단 금지)** 부당한 요금청구에 이의를 제기하는 이용자가 자신의 계정에 접근할 수 있는 정당한 권리를 해치지 않을 것

▶ FTC는 상기 동의명령합의서를 승인한 후 다른 이해관계인으로부터 의견을 청취하기 위해 동의명령합의서와 그에 관한 설명문을 연방행정명령집(Federal Register)에 게재('23.1.4.)

- FTC는 상기 합의서에 대해 '23년 2월 3일까지 총 30일 동안 대중의 의견을 수렴 후 FTC가 이를 최종적으로 채택할지 또는 철회할지 여부를 결정할 예정

3. 스페인 개인정보 감독기구의 Techpump Solutions 행정처분 사례

(1) 서론

▶ 스페인 개인정보 감독기구(Agencia Española de Protección de Datos, 이하 AEPD)는 온라인 사업자 Techpump Solutions SL에 52만 5,000 유로의 과징금을 부과('22.10.31.)

19) 동의명령합의란 '동의명령을 포함한 합의(Agreement Containing Consent Order)'의 약칭으로, 이때 동의명령이란 법위반 혐의를 조사 및 심의하는 과정에서 피심인(Respondent)과의 합의를 통해 위법성에 대한 판단 없이 행정절차로서 문제 사안을 종결하는 제도

- Techpump Solutions는 스페인 북부 아스투리아스 지방의 히혼(Gijón)에 소재하는 사업자로, 성인 콘텐츠를 제공하는 5개 웹사이트를 운영
- 상기 5개 웹사이트가 모두 성인 콘텐츠를 주요 테마로 하고 있음에도 아동의 접근 통제 및 아동 개인정보 처리 관련 동의 메커니즘 구현에 미흡
- 이외에도, 개인정보 처리 원칙, 명확한 동의 획득, 정보 제공의무 등을 준수하지 못한 것으로 드러남

(2) 사실관계

▶ AEPD은 Techpump Solutions의 개인정보보호 실태에 관해 직권으로 조사에 나서 Techpump Solutions가 보유한 웹사이트를 점검

- 주로 웹페이지 접근 및 아동 보호, 개인정보보호 정책, 개인정보 처리. 쿠키 정책 등을 중점적으로 조사

▶ Techpump Solutions가 보유한 웹사이트 대다수는 웹페이지 진입 시 이용자의 연령을 묻는 메커니즘이 존재했으나 제대로 작동하지 않았고, 연령의 진위여부를 확인하는 수단 또한 갖추지 못함

- 성인인지 여부를 묻는 팝업창에 '아니요'를 누르면 메커니즘이 정상 작동하여 웹페이지 접근이 차단되나, 팝업창에 있는 'X'버튼이나 브라우저의 '뒤로가기' 버튼, 혹은 웹페이지의 임의의 장소에 클릭하면 팝업창이 사라지고 웹페이지 접근이 허용
- 웹페이지 상단에 있는 '회원가입' 버튼을 누르면 이용자의 성명, 성별, 도시, 국가, 이메일, 신용카드 정보와 같은 개인정보를 입력할 수 있는 양식이 나타났으나 해당 회원이 입력하는 정보, 특히 연령 정보의 진위 여부를 판별하는 메커니즘은 구현되어 있지 않음

▶ Techpump Solutions의 웹사이트는 회원가입 시 14세 미만 미성년자를 위한 부모 동의 제공 수단을 갖추지 못했으며, 14세 이상의 미성년자의 경우에도 해당 미성년자가 14세 미만인지 혹은 이상인지를 판별하는 메커니즘이 없었음

- 이는 웹사이트가 성인 콘텐츠 제공을 기본으로 하고 있고 웹사이트상의 배너에서도 18세 이상의 성인을 대상으로 서비스를 제공한다는 경고를 표시하고 있는 것과 연관되어 있는 것을 추정

▶ 상기 웹사이트의 개인정보보호 정책은 실제 개인정보 처리 활동과 일치하지 않거나 부당한 경우가 많았음

- 웹사이트의 개인정보보호 정책에는 예외적인 사유를 제외하고는 동일 그룹 내 회사로도 개인정보를 전송하지 않는 것을 원칙으로 한다고 규정했으나 해당 원칙이 지켜지지 않음

- 또한 정책상 개인정보 처리 목적을 설정하지 않거나 보유기간을 별도로 명시하지 않기도 함

▶ 웹사이트 개인정보보호 정책에 쓰인 언어와 개인정보보호 정책 열람 후 개인정보 처리에 관한 동의 제공 인터페이스에도 문제점이 발견

- Techpump Solutions가 스페인에 소재하지만 해당 사업자가 보유한 상기 웹사이트의 개인정보보호 정책은 외국 이용자의 편의성을 고려하여 모두 영어로 구성

- 또한 이용자가 개인정보보호 처리방침을 읽고 동의를 하고자 할 때 동의 제출 양식의 '동의함' 란에 체크가 미리 표기된 채로 화면상에 구현되는 등 적절한 동의 획득 메커니즘이 구현되지 못함

▶ 그밖에, Techpump Solutions는 정보주체에게 정보를 제공할 의무를 소홀히 하거나 정보주체의 권리행사를 어렵게 함과 동시에, 처리 활동 기록 의무를 완전히 수행하지 않음

- 개인정보보호 정책에 공시된 개인정보 처리 목적이 실제 처리 목적과 일치하지 않은 경우가 잦았으나 이와 관련한 정보를 정보주체에게 제공할 의무를 다하지 않음

- 또한, 정보주체가 권리를 행사하는 경우 신분증이나 여권정보와 같은 과도한 개인정보를 제공하도록 요구

- 이외에, 처리 활동 기록 시 반드시 포함해야 할 사항 중 일부를 누락하기도 함

(3) 쟁점 판단(미성년자 보호 관련)

▶ **(적절한 기술적·관리적 보호조치 의무 미준수)** Techpump Solutions는 웹사이트에 접속하는 이용자의 연령이 법적 연령에 도달했는지를 확인하는 적절한 조치를 취하지 못함

- Techpump Solutions는 개인정보보호 정책상 18세 이상의 성인만을 대상으로 서비스를 제한하고 있으므로, 해당 연령대의 정보주체에 대해서만 개인정보 처리가 수행되도록 적절한 기술적·관리적 조치를 구현하는 것도 동 회사의 의무에 해당

  - 따라서, 미성년자의 개인정보가 처리되지 않도록 적절한 기술적·관리적 조치를 구현하는 것 또한 회사의 의무에 속함

- 그러나, 현재 웹사이트는 미성년자가 회원가입을 거치지 않은 경우에도 성인 콘텐츠에 제한 없이 직접 접근할 수 있도록 비정상적으로 작동하고 있으며,
- 회원가입을 거친 미성년자의 경우에도 해당 이용자가 제공한 연령 정보의 진위 여부를 검증할 수 있는 메커니즘을 갖추지 못해 미성년자가 결국 제한 없이 성인 콘텐츠에 접근이 가능
- 따라서 Techpump Solutions는 이용자의 회원가입 여부에 관계없이 웹페이지에 접근하는 이용자의 연령을 적절히 확인함으로써 미성년자를 보호하는 조치를 제대로 구현하지 못한 것으로 나타남

▶ **(미성년자 동의 획득 요건 위반)** Techpump Solutions는 미성년자의 개인정보 처리를 위해 친권자 또는 후견인의 동의를 받았어야 하나 이들이 유효한 동의를 제공하기 위한 메커니즘을 갖추지 못함

- Techpump Solutions가 보유한 일련의 웹사이트는 GDPR상의 '정보사회서비스'로서, 성인을 서비스 제공 대상으로 한정한다는 점을 이용자에게 명시적으로 밝힐 경우 미성년자 개인정보 처리에 관한 동의 획득 여부를 판단할 여지가 없으나,
- 상기 웹사이트는 배너에서는 성인용 웹사이트로서 이용자가 18세 이상이어야 한다고 경고하면서도, 웹사이트 개인정보보호 정책에는 배너와 달리 서비스가 미성년자에게도 제공되는 것처럼 표현하고 있음
  - 개인정보보호 정책에서는 '웹사이트는 성인을 위한 것으로 18세 이상을 대상으로 하기 때문에 14세 미만의 미성년자는 GDPR 제8조에 따라 개인정보 수집 양식에 개인정보를 제공할 수 없다'고 하면서, '미성년자의 동의가 필요한 경우 친권자 혹은 후견인이 승인해야 하며 이에 따라 개인정보를 수집해야 한다'고 규정
  - 이는 곧 해당 서비스가 GDPR의 의미 내에서 14세 미만의 미성년자에게도 직접 제공된다는 것이 명백하고 이러한 이유로 GDPR 제8조가 적용된다고 해석함이 타당[20)]
- 웹사이트의 개인정보보호 정책과 GDPR 제8조의 법문에 따라 상기 웹사이트에는 14세 미만 미성년자의 웹사이트 회원가입과 관련하여 친권자 또는 후견인이 동의를 제공할 수 있어야 함에도 이를 보장하는 메커니즘이 없음
- 반면, 미성년자가 14세 이상인 경우 친권자 또는 후견인의 승인 없이 정보주체의 동의만으로도 개인정보 처리가 가능하므로 컨트롤러인 Techpump Solutions는 해당

20) GDPR 제8조에서는 유효한 동의를 직접 제공할 수 있는 아동의 연령을 16세로 보면서도 EU회원국에 해당 연령을 하향할 수 있는 재량을 부여하고 있으며, 이에 따라 스페인 개인정보보호법에서는 해당 연령을 14세로 낮추어 규정 (스페인 개인정보보호법 제7조)

미성년자가 14세 이상인지 여부를 확인할 수 있는 합리적인 조치를 수립했어야 함

- 그러나 웹페이지에는 회원가입을 시도하는 이용자가 14세 이상인지 여부를 확인하는 수단이 제대로 갖춰지지 않았음

- 결과적으로 14세 미만의 미성년자에 대해서는 친권자 또는 후견인의 동의 제공 수단이 구현되어 있지 않고, 14세 이상의 미성년자에 경우 14세 이상인지 여부를 확인하기 위한 메커니즘이 확립되어 있지 않았다고 볼 수 있음

- 따라서 Techpump Solutions는 정보사회서비스에서의 개인정보 처리에서 아동의 유효한 동의와 관련하여 GDPR 제8조를 위반했다고 결론

(4) 기타 쟁점 판단

▶ **(개인정보 처리 원칙 위반)** Techpump Solutions는 투명성 원칙, 목적 제한 원칙, 보유기간 제한 원칙 등 개인정보 처리 원칙을 위반

- **(투명성 원칙 위반)** Techpump Solutions는 자사의 개인정보보호 정책에 따를 경우 원칙적으로 동일 그룹 내 회사로 개인정보 전송이 발생하지 않았어야 하나 그룹 내 회사로 개인정보의 국외이전이 빈번히 발생했으며 해당 사실을 투명하게 공개하지 않음

- **(목적 제한 원칙 위반)** 동 회사는 개인정보보호 정책에 표현된 처리 목적을 넘어 국가보안이나 세무 등과 같은 다른 목적을 위해 개인정보를 처리한 것으로 드러나 목적 제한 원칙을 준수하지 못함

- **(보유기간 제한 원칙 위반)** 더불어 개인정보보호 정책에는 이용자가 동의 철회를 요청할 때까지 해당 웹페이지를 이용하는 이용자의 개인정보를 무기한 보유하도록 규정하고 있어 필요기간 이상 개인정보를 보유하고자 함

▶ **(처리의 적법성 위반)** Techpump Solutions는 이용자의 개인정보 처리에 대한 동의를 받을 때 명확하고 자발적인 행위를 바탕으로 했어야 하나 미리 '동의함'에 체크 표시가 된 채로 양식을 제공했다면 정보주체의 동의를 적절하게 받은 것이라 볼 수 없음

▶ **(정보 제공 의무 위반 등)** Techpump Solutions는 명확하고 용이한 방식으로 정보주체에게 상세한 정보를 제공해야 할 의무와, 정보주체가 용이하게 권리를 행사하도록 허용해야 할 의무를 위반

- **(GDPR 제12조제1항 위반)** Techpump Solutions는 개인정보보호 정책을 스페인의 공식 언어인 스페인어 대신 영어로 제공하고 있다는 점에서, 스페인 이용자가 이해할 수 있는 방식으로 쉽고 명확하며 단순한 방식으로 정보를 제공했다고 볼 수 없음

- **(GDPR 제13조 위반)** 또한 개인정보보호 정책에 공시된 개인정보 처리 목적이 실제 목적과 불일치한 경우가 많아, 목적 범위를 벗어난 처리 시 GDPR 제13조제1항 제c호에 따라 관련 정보를 정보주체에게 알려야 했음에도 소극적으로 대응했으며, 동법 제7조제3항에 규정된 동의 철회권에 관한 정보도 전혀 제공하지 않음

- **(GDPR 제12조제2항 위반)** 동 회사는 컨트롤러로서 정보주체의 권리 행사를 용이하게 해야 함에도, 권리 행사 시 신분증 및 여권정보 등을 반드시 제공하도록 개인정보보호 정책상에 요건을 규정하는 등 정보주체의 권리 행사를 어렵게 함

▶ **(Data protection by design and by default 위반)** Techpump Solutions는 상기 웹사이트가 가동되기 전, 개인정보 처리의 주기를 감안함과 동시에 어떤 개인정보를 어떻게 처리해야 할 것인지를 설계 단계에서부터 고려하지 않은 채 이용자 개인정보의 처리를 시작

▶ **(처리 활동 기록 의무 위반)** Techpump Solutions는 처리 활동 기록 의무를 제대로 준수하지 않음

- 컨트롤러는 처리 활동 기록 시 세부적으로 ▲컨트롤러 등의 이름, 연락처 ▲처리 목적 ▲정보주체의 범주 및 개인정보의 범주에 대한 설명 ▲GDPR 제32조제1항에 규정된 기술적 관리적 보안조치에 대한 설명 등을 모두 포함했어야 하나 처리 목적 중 일부를 포함하지 않거나 구체적 설명을 누락

(5) 제재

▶ **(과징금 부과)** AEPD는 상기와 같은 일련의 개인정보보호 위반행위에 대해 GDPR 제5조제1항제a호, 제b호 및 제e호, 제6조제1항, 제12조제1항 및 제2항, 제13조, 제25조, 제30조 위반 등을 이유로 52만 5,000 유로의 과징금을 부과

▶ **(시정명령 부과)** 또한 AEPD는 행정처분 결정 발표 후 1개월 이내에 Techpump Solutions에 시정조치를 이행하도록 명령하고 이행된 조치를 AEPD에 통보할 것을 요구

Reference

1. AEPD, Procedimiento Nº: PS/00555/2021, 2022.10.31.
2. Dataguidance, Spain: AEPD fines Techpump Solutions €525,000 for data processing violations, 2022.11.2.
3. Edora Consulting, Sanción de 525.000€ al titular de webs de contenido para adultos por varios incumplimientos en LOPD, 2022.11.2.
4. Federal Register, Epic Games, Inc.; Analysis of Proposed Consent Order To Aid Public Comment, 2023.1.4.
5. FTC, Agreement Containing Consent Order (In the Matter of EPIC GAMES, INC., a corporation), 2022.12.19.
6. FTC, Complaint (In the Matter of EPIC GAMES, INC., a corporation), 2022.12.19.
7. FTC, Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges, 2022.12.19.
8. Letslaw, AEPD penalizes a company that owns adult content websites for unlawful use of personal data 2022.12.23.
9. Techlaw, Spanien: Techpump Solutions bötfälls med 525 000 euro för olaglig behandling av personuppgifter, 2022.11.8.
10. United States District Court for the Eastern District of North Carolina, Complaint for Permanent Injunction, Civil Penalties, and Other Relief (USA v. Epic Games, Inc.), 2022.12.19.
11. United States District Court for the Eastern District of North Carolina, Stipulated Order for Permanent Injunction and Civil Penalty Judgment (USA v. Epic Games, Inc.), 2022.12.19.
12. 개인정보보호위원회, 아동청소년 개인정보 보호 가이드라인, 2022.7.21.
13. 한국언론진흥재단, 2022 10대 청소년 미디어 이용 조사, 2022.11.30.

〈2023년 개인정보보호 월간 동향 보고서 발간 목록〉

번호	호수	제 목
1	1호 01	주요국 개인정보보호 강화기술 정책동향 분석 및 시사점
2	1호 02	인공지능법(안)과 GDPR의 상호작용 분석
3	1호 03	해외 아동 개인정보 침해 관련 행정처분 사례 분석

2023
개인정보보호 월간동향분석 제1호

발 행 2023년 2월 3일

발행처 한국인터넷진흥원
전라남도 나주시 진흥길 9
Tel: 061-820-1899