2023 Privacy Report

개인정보보호 월간동향분석

12월호

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2023 Privacy Report

개인정보보호 월간동향분석

12월호

1. 개인정보보호 분야 국제조직(IAPP/GPA/FPF) 주요 활동 및 논의 내용 분석

2. 2023 하반기 주요 개인정보보호 위반에 대한 해외 주요국 제재 및 처분 동향

3. 2023년 국내외 개인정보 이슈 점검과 2024년 주요 이슈 전망

KISA

개인정보보호 분야 국제 조직(IAPP/GPA/FPF) 주요 활동 및 논의 내용 분석

[목 차]

1. 개요

▶ 코로나19 이후 생성형 AI(Generative AI) 관련 서비스들이 급속히 확산하고 AI 기술의 개인정보 침해 위험 등에 대한 우려가 증폭되면서 국제적으로 개인정보보호 거버넌스에 대한 논의 증가

- 의료, 고용 분야 등 AI 기술의 활용이 증가하는 분야에서 신흥 기술 이용에 따른 개인정보보호 관련 기술적, 법률적, 윤리적 위험에 대한 우려 확산
- 국제적으로 개인정보 거버넌스, 생성형 AI 분야에서 개인정보보호 방안 등에 대한 논의가 증가하고, 유럽연합(EU)의 AI 법(안)의 제정 추진에 따른 개인정보보호 수요 증가 전망

▶ '23년에 개인정보보호 분야의 국제기구 및 협의체들은 개인정보보호 현황을 파악하고, 다양한 이해관계자들이 참여하는 심포지엄 등에서 이슈를 논의하며, 기술적·관리적 대응 방안을 개발하고, 결의안 채택 등 개인정보보호 강화 방안을 마련

- IAPP(International Association of Privacy Professionals)는 '23년 11월 개인정보보호 관련 주요 영역 현황 분석을 담은 개인정보보호 거버넌스 연례 보고서 발행
- GPA(Global Privacy Assembly)는 '23년 10월 제45차 GPA 회의에서 GPA의 전략계획(2023~2025), 생성 AI 시스템, 인공지능 및 고용, 의료데이터 및 과학 연구 등 여러 영역에서 결의안을 동시에 채택
- FPF(Future of Privacy Forum)는 '23년 11월 14일 제7차 브뤼셀 개인정보보호 심포지엄(Brussels Privacy Symposium 2023)을 개최하고, EU AI법(안), 디지털 서비스법(DSA), 디지털 시장법(DMA)의 주요 원칙과 데이터 전략의 기타 관련 법률 등에 대해 논의

2. IAPP(International Association of Privacy Professionals)

(1) IAPP-EY 2023 개인정보보호 거버넌스 연례 보고서

▶ IAPP는 '23년 11월, '2023 개인정보보호 거버넌스 연례 보고서(IAPP-EY Annual Privacy Governance Report 2023)'를 발행[1)]

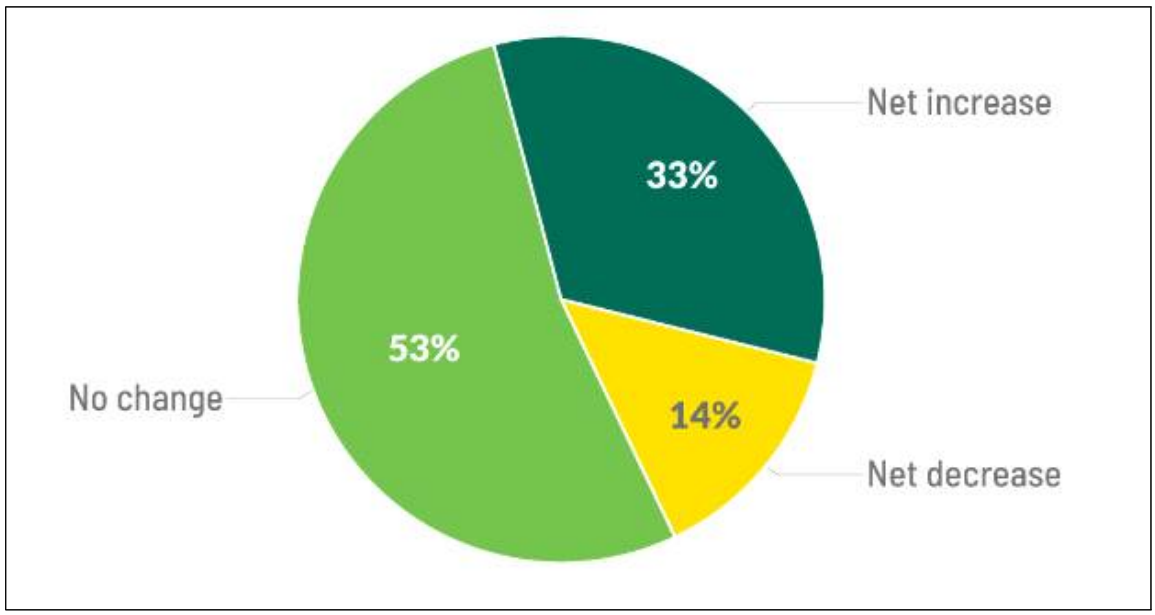
- 동 보고서는 개인정보보호 관련 컴플라이언스, 개인정보보호 전략, 보고 체계, 개인정보보호 기능, DPO, 감독기관 예산, 새로운 위험관리, 기술기반 컴플라이언스, 수행 척도 등과 관련한 설문조사 결과를 분석

▶ (주요 내용) 개인정보보호 거버넌스 연례 보고서의 주요 내용은 같음

- 지난 한 해 동안 조직의 33%는 어려운 경제 상황에서도 개인정보보호 담당팀이 성장한 것으로 확인
  - 개인정보보호 전문가와 개인정보보호 팀의 역할이 일상적 조직 운영과 전략계획의 모든 측면에서 확장하고 통합하면서 조직의 개인정보보호 투자가 증가
  - 오늘날 개인정보보호 기능은 정보 경제에서 데이터 중심이 되면서 조직에서 중요한 기능을 수행

1) IAPP, IAPP-EY Annual Privacy Governance Report 2023, 2023.11.; https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2023_Executive_Summary.pdf

그림 _ '23년도 개인정보보호팀의 변경(성장)



출처: IAPP('23.11)

- 설문 조사에 참여한 개인정보보호 전문가 중 86%는 조직 내에서 3개 이상의 팀과 정기적으로 협력하고 있다고 응답

  - 의사 결정은 최고위층에서 이루어지며, 조사 대상자의 50% 이상이 회사의 최고 경영진에게 직접 보고한다고 응답했으며, 78%는 최고 개인정보보호 책임자가 조직의 최고 5개 직급에 속한다고 응답

- 개인정보보호 및 관련 규정에 대한 정보를 쉽게 이용 가능

- 응답자의 96% 이상은 새로운 개인정보 보호법 및 정책 이니셔티브에 대한 정보를 지속적으로 확보할 수 있다고 확신

  - 개인정보보호의 중요성이 명확한 상황이나, 해당 분야에 대한 심층적 이해를 원하는 사람들에게는 정보가 부족

- 글로벌 개인정보보호 규정 및 표준을 준수하는 것이 성공에 중요하다는 인식에도 불구하고 예산 제약으로 인해 개인정보보호 거버넌스의 효율성에 대한 조직의 신뢰는 위협받고 있음

  - 응답자 중 63%는 조직 내 한정적 자원(인력, 예산 등)이 개인정보보호 목표 달성을 저해하는 영향을 끼칠 수 있다고 응답

  - 응답자 중 63%는 현재 채용이 진행되고 있지 않다고 응답했으며, 67%는 예산이 충분하지 않다고 응답

- 조사 대상자 중 10명 중 2명만이 조직의 개인정보보호법 준수에 대해 전적으로 확신한다고 응답

- 더 적은 비용으로 더 많은 일을 해야 하는 상황에서 스마트한 작업 방식을 요구하며, 이에 따라 개인정보보호강화기술(PET) 등에 대한 교육 및 기술 투자의 중요성 커질 전망

• 개인정보보호에 대한 자신의 권리를 점점 더 인식하는 소비자는 적절한 권리 보호가 없는 경우 대체 제품 및 서비스를 선택할 수 있음

- 개인정보보호 규정을 준수하지 못하는 조직들은 수십억 달러에 달하는 과징금, 소비자 불신, 비즈니스 모델 붕괴 및 시장 폐쇄를 경험할 수 있음

3. GPA(Global Privacy Assembly)

▶ '23년 10월 제45차 GPA 회의에서 다음과 같은 여러 중요한 결의안을 채택

• GPA의 전략계획(2023~2025)에 관한 결의안(Resolution on the GPA's Strategic Plan (2023-2025)

• 생성형 AI 시스템에 관한 결의안(Resolution on Generative Artificial Intelligence Systems)

• 인공지능 및 고용에 관해 아래와 같은 결의안(Resolution on Artificial Intelligence and Employment)

• 의료데이터 및 과학 연구에 관한 아래 사항을 담은 결의안

▶ GPA의 전략계획(2023~2025)에 관해 아래 사항은 담은 결의안(Resolution on the GPA's Strategic Plan (2023-2025) 채택[2)]

• (전략목표) 3대 전략목표(▲글로벌 프레임워크에서 높은 수준의 개인정보보호 ▲ 전략적 제휴 및 영향력 ▲ DPA 역량 강화) 설정

2) GPA. Resolution on the GPA's Strategic Plan (2023-2025), 2023.10.; https://edps.europa.eu/system/files/2023-10/gpa-strategic-plan-final-version-update_en.pdf

표 1_ 전략목표의 결과

전략목표	전략목표의 결과
글로벌 프레임워크에서 높은 수준의 개인정보보호	• 높고 일관된 수준의 개인정보보호를 통해 글로벌 프레임워크 개발에 영향을 주고 지원하며 표준과 모델을 만드는 데 기여 • 기술 혁신을 위한 윤리적 원칙을 강화 • 개인정보보호 표준 및 프레임워크 시행 협력을 극대화 • 신흥기술을 개발하고 사람들에게 권한을 부여하기 위해 PET의 사용 장려
전략적 제휴 및 영향력	• 다른 국제 그룹 및 포럼에서 실무 그룹의 참여를 늘려 GPA의 외부 참여를 강화 • GPA와 국제 및 지역 조직 간의 의사소통 채널을 강화 • 외부 이해관계자(타 부문별 규제 기관, 과학 및 학술 부문 등)의 GPA 참여 강화 • GPA 거버넌스 개선
개인징보감독기관(DPA) 역량 강화	• DPA 간 경험, 전략, 모범사례를 공유하여 학습 공간을 강화 • DPA와 개인 간 대화와 교육을 위한 공간을 만들어 개인정보보호를 위한 도구와 전략을 공유 • 정보주체의 권리를 강화 • GPA 현대화하려는 의도를 지원하기 위해 GPA 유료 사무국을 운영

출처: GPA('23.10)

• (운영계획) 실행 및 작업반(Actions and working groups)별로 구체적인 운영계획을 마련

표 2_ 실행 및 작업반 운영계획

실행 및 작업 그룹	운영계획 주요내용
국제 개발 원조, 국제 인도주의적 지원 및 위기관리에서 개인정보보호(AIDWG)	• 다른 조직과 협력하여 PDP(Privacy & Data Protection)에 대한 인식 캠페인을 촉진 • PDP와 관련된 문제를 해결하기 위해 다른 조직 및 네트워크와 공동 조치를 취함 • 취약한 커뮤니티의 개인정보보호를 다루는 문서를 작성
글로벌 프레임워크 및 표준(GFSWG)	• 전 세계적으로 높고 일관된 수준의 개인정보보호를 위한 일반 원칙을 설정하기 위해 현재까지 수행된 GPA 작업을 장려 • 개인정보의 국제 전송을 위한 다양한 메커니즘에 대한 추가 비교 분석 수행을 고려 • 국경 간 전송에 관해 해당 관할권 내 GPA 회원 및 조직의 문제, 우려 및 요구사항을 식별하고 해결하기 위한 활동이 무엇인지 고려
인공지능의 윤리 및 개인정보보호(AIWG)	• 신흥 기술의 윤리 원칙 구현에 대한 DPA의 경험을 강조 • 신흥 기술에 직면한 개인정보보호 문제에 대한 전시 및 토론 공간 마련 • AI와 같은 최신 기술의 사용에 관해 정보주체를 위한 권장 사항이 포함된 홍보 자료를 개발 • 생성 AI 시스템에 대한 후속 작업 수행

실행 및 작업 그룹	운영계획 주요내용
데이터 공유 작업반(DSWG)	• 데이터 공유에 대한 국제 규제 프레임워크를 분석하는 비교 연구 수행 • 민간 부문과 공공 부문 간의 데이터 교환을 위한 매뉴얼 또는 모범사례 가이드. 개발
국제 집행 협력(IECWG)	• 보다 성숙한 당국의 집행 경험을 배우고 개인정보보호법 집행 협력을 촉진하는 이니셔티브(예: GPA 워크숍)를 통해 역량 구축을 촉진 • 개인정보보호 영역에서 다른 작업반 및 기타 지역 또는 국제 네트워크와 같은 이해관계자와 시너지 효과를 창출 • 개인정보보호의 글로벌 시행을 최적화하기 위한 협력 기회를 식별 • 전 세계적으로 관련성이 있고 우려되는 개인정보보호 문제에 대한 비공개 세션을 계속 • 기존 주제 하위 그룹(예: 애드테크, 사이버보안, 데이터 스크래핑, 얼굴 인식 기술, 스마트 안경)의 협력 이니셔티브를 지속
개인정보보호 및 기타 권리 및 자유(DPORFWG)	• 2024년 첫 번째 수상을 위해 새로운 GPA 개인정보보호 및 인권상 프로그램을 시험 • GPA 회원들이 PDP에 대한 문서 및 자료를 생성하도록 권장 • PDP 및 기타 기본권과의 관계를 연구하는 학술 기관과 협력 • 기본권과의 연계에 관해 PDP 커뮤니티 내에서 토론을 촉진 • GPA 회원들이 개인정보보호와 기타 권리 사이의 교차점 연구
디지털 시민 및 소비자(DCCWG):	• 소비자 보호, 경쟁 및 독점 금지 관점뿐만 아니라 PDP의 위험과 기회를 더 잘 이해하기 위해 학계, 기타 이해관계자와 협력 • 개인정보보호, 경쟁 및 독점 금지, 소비자 보호 및 기타 교차하는 규제 영역 간의 교차 사례의 연관성 매칭 • 규제 장애물을 식별 • DPA와 기타 규제 당국 간 협력을 장려하고 촉진
디지털 교육(DEWG)	• 아동 및 청소년의 개인정보침해 가능성에 직면하여 불만 사항의 수리 또는 주의를 위한 메커니즘을 구축하거나 기관 행위자와 다른 채널을 통해 집행기관을 지원 • 어린이와 청소년의 개인정보보호 및 PDP에 대한 인식 캠페인을 촉진 • 교육 전문가가 개인정보보호, 개인정보보호 인식 및 교육을 통해 청소년에게 디지털 시민의식을 교육하는 데 필요한 역량을 갖추도록 보장 • 투명하고 아동 친화적인 PDP 정책을 위해 이해관계자에게 영향을 미칠 수 있도록 파트너 조직과 공동의 조치 수행
디지털 경제(DEWG)	• 개인정보보호에 대한 감시 기술의 영향을 다루는 조치 또는 제품 생성 • 보안 위반이 발생 시 개인정보보호 기관에서 수행하는 조치 과정 식별 • 이러한 경험을 요약한 절차 매뉴얼을 개발
개인정보보호 지표(DPMDWG)	• 작업반의 관리 지표 작성을 지원 • 2023-2025년 전략계획 지표에 대한 후속조치를 수행 • WG의 결의사항 준수 진행 상황에 대한 측정을 수행

출처: GPA('23.10)

▶ 생성형 AI 시스템에 관해 아래 사항을 담은 결의안(Resolution on Generative Artificial Intelligence Systems) 채택[3)]

- 적용할 수 있는 원칙과 권리를 포함하여 생성형 AI 기술의 맥락에서 개인정보보호 및 개인정보보호법의 적용 및 집행을 보장하기로 약속함
- 윤리적, 법적, 사회적, 기술적 관점에서 생성형 AI의 맥락 내에서 개인정보보호를 보장하기 위해 협력하기로 약속함
- 윤리 및 개인정보보호 내에서 생성형 AI 시스템의 개인정보보호 및 개인정보보호 위험과 관련하여 관할권 내에서 진행 중인 개발을 공유하기로 약속함
- 생성형 AI 시스템의 개발자, 제공자 및 배포자에게 개인정보보호를 기본 인권으로 인식하고 인간 존엄성 및 기타 기본 권리와 자유를 보호하는 책임감 있고 신뢰할 수 있는 생성형 AI 기술을 구축할 것을 요청함
- 생성형 AI 시스템의 개발자, 제공자, 배포자가 개인정보보호, 정보주체 권리와 관련하여 생성 AI 시스템의 개발 및 배포를 이해할 수 있도록 직원하고, 인력교육을 제공하도록 권장
- GPA 회원들이 개인정보보호, 기타 인권에 대한 위험뿐만 아니라 생성형 AI 시스템의 맥락에서 개인정보보호 및 해당 법적 의무 및 원칙에 대한 인식을 높이도록 권장함
- 생성형 AI의 맥락에서 발생하는 기본 권리와 자유에 대한 새로운 위험과 잠재적 피해를 계속 모니터링 수행함
- 진행 중이거나 향후 입법 및 규제 계획과 접근법을 지지하고 조언함
- GPA 회원에게 생성형 AI 시스템에 대한 집행 노력을 조정하도록 요청함
- 제46차 GPA 총회에서 생성형 AI 시스템의 작업에 대한 중간보고서 제출을 고려하고, 제47차 GPA 총회에서 발표할 추가 정책 문서 또는 결의안을 추가로 고려함

▶ 인공지능 및 고용에 관해 아래와 같은 결의안(Resolution on Artificial Intelligence and Employment) 채택[4)]

- 고용 맥락에서 사용할 AI 시스템을 개발하거나 사용하는 조직이 본 결의안에 설명된 고려 사항을 검토할 것을 촉구함

3) GPA. Resolution on Generative Artificial Intelligence Systems, 2023.10.: https://globalprivacyassembly.org/wp-content/uploads/2023/10/5.-Resolution-on-Generative-AI-Systems-101023.pdf
4) GPA, Resolution on Artificial Intelligence and Employment, 2023.10.: https://globalprivacyassembly.org/wp-content/uploads/2023/10/1.-Resolution-on-AI-and-employment-1.pdf

- GPA의 모든 구성원에게 관할권 및 전 세계 고용에서 사용할 AI 시스템을 개발하거나 사용하는 조직과 협력하여 결의안에 설명된 고려 사항을 통합할 수 있도록 요청함
- 채용에서 인공지능의 사용에 대한 기술적 및 법적 상황이 변경되는 경우에서 인공지능의 윤리 및 개인정보보호에 관한 실무반의 조사 결과에 대한 현행화를 수행함

▶ 의료데이터 및 과학 연구에 관한 아래 사항을 담은 결의안(Resolution on health data and scientific research) 채택[5]

- 과학적 목적 또는 연구 맥락에서 개인의 의료데이터를 수집하고 처리하는 데 관여하는 모든 의사 결정자, 이해관계자가 개인정보보호 설계를 장기간에 걸쳐 연구 프로젝트 설계의 핵심 요소로 수용하도록 요청
- GPA 데이터 공유 작업반에 과학적 목적 또는 연구 맥락에서 의료데이터의 수집 및 처리를 다루는 것에 대해 더 깊이 숙고하도록 요청

4. FPF(Future of Privacy Forum)

▶ 개인정보보호에 중점을 둔 글로벌 비영리 단체인 FPF는 VUB(Vrije Universiteit Brussel)의 브뤼셀 개인정보보호 허브가 공동으로 '23년 11월 14일 제7차 브뤼셀 개인정보보호 심포지엄(Brussels Privacy Symposium 2023 개최[6]

- 브뤼셀에서 정책입안자, 학계 연구원, 시민 사회 및 업계 대표가 모여 실용적이고 적용할 수 있으며 실질적인 개인정보보호 연구 및 학문을 공유
- 올해 주제인 'EU 데이터 전략 아키텍처의 이해: 공통 스레드–접점– 불일치("Understanding the EU Data Strategy Architecture: Common Threads – Points of Junction – Incongruities)'에 따라 참가자들은 다가오는 EU AI 법, 디지털 서비스법(DSA), 디지털 시장법(DMA)의 주요 원칙과 관련 법률 논의

5) GPA. Resolution on health data and scientific research 2023.10.; https://globalprivacyassembly.org/wp-content/uploads/2023/10/Resolution-Health-Data.pdf
6) FPF, Brussels Privacy Symposium 2023. 2023.11.; https://fpf.org/fpf-event/brussels-privacy-symposium-2023/

▶ 제7차 브뤼셀 개인정보보호 심포지엄의 주요 세션과 주요 내용은 다음과 같음

표 3_ 전략목표의 결과

주요 세션	주요 내용
패널 1 **패러다임의 전환**	• 데이터가 개인적인 것인지 여부에 관계없이 데이터에 대한 접근을 촉진하는 것이 데이터 전략 패키지의 주요 주제일 수 있음 - 디지털 서비스법(DSA)에 따라 당국에 데이터에 대한 액세스를 제공하기 위해 대규모 온라인 플랫폼에 대한 특정 법적 요구사항을 포함 - 디지털 시장법(DMA)에 따라 게이트키퍼에게 광범위한 실시간 데이터 이동성 의무와 상호운용성 의무를 부과 - 데이터 거버넌스법(DGA)에 따라 공공 기관이 보유한 데이터에 대한 접근을 촉진하고, 데이터를 수집하기 위한 전문적인 유럽 데이터 공간을 구축
패널 2 **영향평가 네트워크: GDPR에서 DSA 및 AI 법까지**	• DSA 제34조와 같은 주요 EU 디지털 규정에 포함된 다양한 위험 기반 영향평가 조항과 EU AI법(안)의 기본권 영향평가를 조명 • 개인정보보호 영향을 평가하기 위해 새로운 법안과 GDPR 35조 사이의 교차점을 탐색하고 유럽(네덜란드 등)에 이미 존재하는 인권 영향평가 모델을 탐색 • 현장 전문가가 참여하여 EU 디지털 규제의 진화하는 영역 전반에 걸쳐 영향평가에 대한 접근 방식과 이해관계자에게 미치는 영향 이해를 제공 - 다양한 유형의 영향평가, 상호 연결성 및 GDPR과의 관계에 대해 학습하는 기회를 제공하고 영향평가를 수행하기 위한 주요 고려 사항에 대해서도 논의
패널 3 **유럽의 데이터 시행의 미래**	• 원스톱 숍(One-Stop-Shop) 하의 협력 및 일관성 메커니즘을 갖춘 GDPR은 EU 법률에서 가장 복잡하고 다층적인 집행 구조 중 하나를 만들었음 - 실제로 GDPR이 적용되고 5년 후, EU집행위원회는 주로 국가 행정 절차 수정을 고려하여 이 시스템을 개혁하기 위한 새로운 규칙을 제안함 - 데이터 전략 입법 패키지를 통해 EU 입법자는 초점을 전환하고 EU 회원국 전체에 분산된 집행 모델에 중앙 집중식 집행 모델을 추가 • 데이터 전략 패키지는 데이터, 알고리즘, AI 및 디지털 세계에 대해 말할 수 있는 국가 감독기관의 네트워크를 크게 향상 • 개인정보보호 당국은 데이터 전략 패키지에 포함된 다른 모든 법률의 적용 범위를 뒷받침하는 처리를 포함하여 개인 데이터의 모든 처리를 계속해서 처리 • 최근 유럽 법원의 판결에서 독점금지 당국이 개인정보 처리와 관련된 문제를 기반으로 자체 판단을 내릴 수 있는 능력을 확인

출처: FPF('23.11)

5. 결론 및 시사점

▶ 국제적으로 생성 AI 기술 등 신흥 기술의 확산으로 개인정보보호 침해 우려가 확산되면서 개인정보보호 분야의 국제기구 및 협의체는 관련 기술적, 관리적, 법제적 관점에서 이해관계자 논의 및 대응 방안들을 제시

- IAPP의 경우 '23년 주요 개인정보보호 영역에 대한 현황 분석
- GPA 제45차 GPA 회의에서 GPA의 전략계획(2023~2025), 생성 AI 시스템, 인공지능 및 고용, 의료데이터 및 과학 연구 등 여러 영역에서 결의안을 채택
- FPF 제7차 브뤼셀 개인정보보호 심포지엄(Brussels Privacy Symposium 2023에서 EU AI법(안), 디지털 서비스법(DSA), 디지털 시장법(DMA)의 주요 원칙과 법률 등에 대해 논의

▶ '23년에는 생성 AI의 부상으로 유럽은 AI 법안의 입법화를 추진하고, 국제기구 등은 개인의 권리를 보호하고 안전하고 책임감 있는 AI 개발과 보급을 위한 가이드라인 개발과 원칙을 마련하고 있으며, 이에 따른 국내에서도 개인정보보호 분야의 국제적인 협력을 강화하고, 개인정보보호에 대한 투자 강화 필요

- EU의 GDPR은 물론 AI 법안 등 국제적인 개인정보보호 관련 규범에 대한 영향을 분석하고, 신흥 기술의 개인정보 침해 위험 분석과 PET 고도화 및 보급 필요
- 국내 개인정보보호 전문가들의 국제기구 및 협의체의 참여를 확대하여 개인정보보호 관련 기술적, 법률적 대응이나 경험 등을 공유하고, 생성 AI 등 새로운 기술에 대한 위험을 완화하기 위한 개인정보보호 규범이나 지침 개발에서 공동 협력 강화 필요

Reference

1. FPF, Brussels Privacy Symposium 2023. 2023.11.
2. GPA. Resolution on the GPA's Strategic Plan (2023-2025), 2023.10.
3. GPA. Resolution on Generative Artificial Intelligence Systems, 2023.10.
4. GPA, Resolution on Artificial Intelligence and Employment, 2023.10.
5. GPA. Resolution on health data and scientific research 2023.10.
6. IAPP, IAPP-EY Annual Privacy Governance Report 2023, 2023.11.

2023년 하반기 주요 개인정보보호 위반에 대한 해외 주요국 제재 및 처분 동향

[목 차]

1. 개인정보보호 규정 위반 및 과징금 부과 사례 동향

▶ EU 일반 개인정보보호법(GDPR) 시행('18.5.) 이후 EU 각국의 개인정보 감독기관(Data Protection Authorities, 이하 DPA)들은 GDPR 위반 혐의에 대한 민원을 접수해 조사하고 있으며, 위반 사실이 확인될 경우 과징금 부과와 함께 제재를 가하고 있음

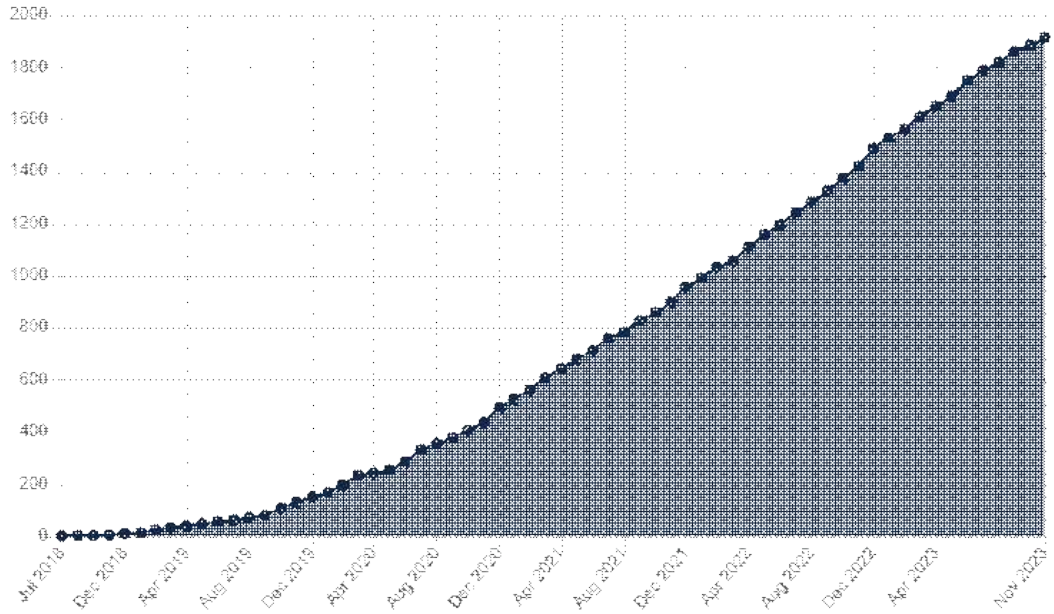
- EU 국가들은 '18년 GDPR 시행 이래 '23년 11월[7]까지, 총 1,914건의 규정 위반 사례에 대해 총 44.2억 유로의 과징금을 부과
- GDPR 위반 사례 월 최대 위반 적발 건수는 67건('22.12.)이었으며, 평균적으로 매월 30~50건의 위반 사례가 지속적으로 적발되고 있는 상황

7) 현재('23년 12월) 기준 독일 법무법인 CMS에서 공개한 개인정보보호 행정 처분 관련 통계는 '23년 11월까지의 과징금 부과 건을 반영하여 집계하고 있음. https://www.enforcementtracker.com/?insights 참고

- 특히 '22년~'23년 사이 대규모 과징금 부과 사례가 증가하여 현재까지 건당 1,000만 유로 이상의 과징금을 부과한 사례가 33건이며, 이 중 1억 유로 이상의 과징금을 부과한 사례는 11건에 이르고 있음

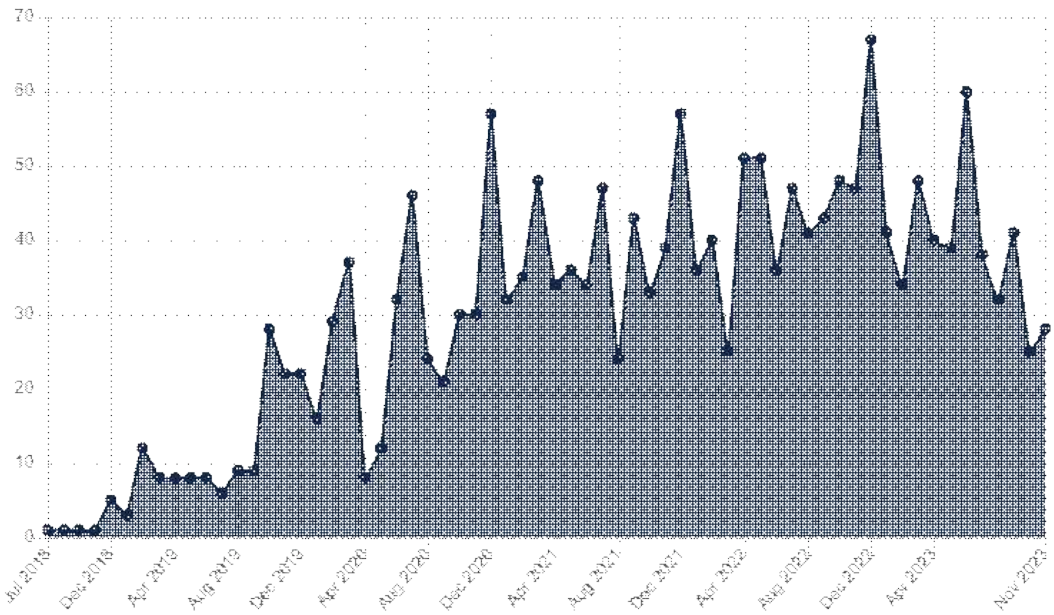
* 현재까지 가장 큰 규모의 과징금 부과 사례는 '23년 5월 아일랜드 개인정보 감독기관(Data Protection Commission, 이하 DPC)이 Meta Platforms Ireland Limited에 부과한 사례로, 부과 과징금이 12억 유로에 달함

그림 1_ GDPR 위반 사례 전체 누적 건수('18.7월~'23.11월)



출처: CMS.Law, GDPR Enforcement Tracker

그림 2_ 월별 GDPR 위반 과징금 부과 건수(비누적) ('18.7월~'23.11월)



출처: CMS.Law, GDPR Enforcement Tracker

▶ 위반 사례 유형별로는 개인정보 처리를 위한 법적 근거 미비가 607건으로 가장 많았으며, 이어서 ▲일반 개인정보 처리 원칙 미준수(533건) ▲정보보안을 위한 기술적·조직적 조치 미비(349건) ▲정보주체 권리 보장 의무 위반(188건) ▲정보 제공 의무 미준수(184건) 순

▶ 한편 과징금 규모 면에서는 일반 개인정보 처리 원칙 미준수가 약 20억 3,659만 유로의 누적액으로, 타 규정 위반 대비 압도적으로 높은 수준으로 나타남

표 1_ GDPR 위반 유형별 건수 및 과징금 규모

위반 유형	과징금 부과 건수	과징금액(백만 유로)
개인정보 처리의 법적 근거 미비	607	1,649.0
일반 개인정보 처리 원칙 미준수	533	2,036.5
정보보안을 위한 기술적·조직적 조치 미비	349	385.1
정보주체 권리 보장 의무 위반	188	98.1
정보 제공 의무 미준수	184	237.3
감독기관과의 미협조	92	6.1
개인정보 침해 통지 의무 이행 미비	32	1.7
DPO 참여 미비	15	0.9
개인정보 처리 계약 관련 위반	11	1.0
기타	9	9.2

출처: CMS.Law, GDPR Enforcement Tracker

▶ 한편 GDPR 시행 이후 EU 외의 국가들도 자국의 상황에 적합한 개인정보보호 법령 정비에 본격적으로 나서고 있으며, 각국 개인정보 감독기관들은 개인정보 침해에 대해 대규모 과징금을 부과하는 등 적극적인 집행을 이어가는 추세임

- 미국 연방거래위원회(FTC)는 사용자를 속여 원치 않는 결제를 유도한 것에 대해 게임 개발사 에픽게임즈(Epic Games)와 2억 4,500만 달러(약 3,215억 6,250만 원) 합의('23.3.)[8]
- 중국 국가인터넷정보판공실(CAC)은 '23년 9월, 중국 최대 학술 데이터베이스인 China National Knowledge Infrastructure(CNKI)에 개인정보 무단 수집 및 처리에 대해 과징금 5천만 위안(약 91억 250만 원)을 부과[9]

8) https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-finalizes-order-requiring-fortnite-maker-epic-games-pay-245-million-tricking-users-making, https://www.dataguidance.com/news/usa-ftc-finalises-order-against-epic-games-privacy
9) https://www.reuters.com/article/china-regulation-cnki/update-1-china-cybersecurity-authority-fines-chinese-academic-database-cnki-50-mln-yuan-idINL1N3AI0MD

- 국내에서는 개인정보보호위원회(개인정보위)가 허술한 시스템 보안 및 개인정보 관리로 29만여 건의 개인정보를 유출한 LGU+에 68억 원의 과징금을 부과('23.7.)

  - 이외에 현재 개인정보위가 개인정보보호법 위반과 관련해 소송 진행 중인 과징금·과태료 합산액은 도합 1,090억 원에 달함

▶ 이하에서는 '23년 한 해 발생한 주요 개인정보보호 규정 위반 및 과징금 부과 사례를 살펴보고, 이들 사례를 중심으로 위반 특징과 시사점을 제시하고자 함

2. 글로벌 개인정보보호 규정 위반 및 과징금 부과 사례 분석

(1) 미국 FTC, COPPA 및 FTC법 위반 혐의로 Epic Games에 5억 2,000만 달러 부과

① 개요

▶ 인기 게임 포트나이트(Fortnite) 제작사 Epic Games는 개인정보보호 위반 및 원치 않은 요금 청구에 대해 도합 5억 2,000만 달러를 지불하기로 FTC와 합의

- FTC는 ▲아동온라인프라이버시보호법(COPPA, Children's Online Privacy Protection Act)을 위반한 혐의와 관련하여 2억 7,500만 달러 과징금 합의('22.12.) ▲다크패턴 관련 2억 4,500만 달러 과징금 합의('23.3.)를 발표

- 이 중 '23년 3월 합의에 근거해 Epic Games가 지급한 2억 4,500만 달러는 부당한 요금 청구로 피해를 입은 사용자들에 대한 환불 용도로 사용될 예정

▶ '17년부터 '22년까지의 기간 동안 Fortnite에서 성희롱을 포함한 아동 괴롭힘과 학대에 대한 신고가 접수되었으며, FTC는 '22년 12월, 인기 게임사 Epic Games를 상대로 미국 노스캐롤라이나주 동부 지방법원에 소를 제기

- FTC를 대신하여 법무부가 제출한 제소장은 Epic Games가 COPPA에서 규정한 부모 또는 보호자 통지, 동의, 검토 및 삭제 요건을 준수하지 않았으며, Fortnite 게임 내 음성 및 문자 채팅 기본 설정이 유해하고, 불공정적이며, 기만적이라 주장

▶ 이와 별도의 행정조치 및 합의를 통해 FTC는 Epic Games가 모든 연령대의 사용자가 의도하지 않은 게임 내 구매를 유도하고자 다크패턴*을 사용했다고 밝힘

- 제소장에 따르면 Epic Games는 이와 같은 게임 내 무단 청구에 대해 신용카드 회사에 이의를 제기한 고객의 계정을 잠금

② 주요 위반 사항

▶ **(아동 보호 위반)** Epic Games는 아동 사용자 가입과 관련해 부모에게 통지하거나 동의를 얻지 않아 COPPA를 위반했으며, 아동 및 청소년을 대상으로 실시간 문자 및 음성 채팅을 기본 활성화하여 FTC법 제5조를 위반

- Epic Games는 다양한 경로를 통해 13세 미만의 아동이 Fortnite를 이용하고 있다는 사실을 인지하고 있었으나, '19년 말까지 아동 사용자에 대한 부모의 동의를 얻으려고 시도하지 않음
- 예컨대, Epic Games는 10세~12세 미국 아동의 53%가 매주 Fortnite 게임을 즐기고 있다는 공개 설문조사 사본을 받아 본 것을 확인
- 그러나 Epic Games는 13세 미만 아동 개인정보(사용자 이름, 이메일 주소, IP 주소 등)를 수집하면서 부모 또는 보호자로부터 동의를 얻지 않았으며, 이는 COPPA의 동의 및 통지 요건을 위반한 것
- FTC는 ▲부모가 자녀의 개인정보 삭제를 요청하기 위해서는 IP주소, 자녀의 계정 생성 날짜, 구매가 이루어진 위치정보 등 정보를 제공해야 했으며 ▲많은 경우 부모들의 요청이 받아들여지지 않거나 처리되지 않았기에, Epic Games가 COPPA에서 규정한 삭제 요건을 위반했다고 주장
- 아울러, Epic Games가 기본적으로 실시간 음성 및 문자 채팅을 활성화했기에 아동 사용자는 Fortnite 게임을 플레이하는 동안 온라인에서 낯선 사람들과 연결되었으며, 일부의 경우 협박, 괴롭힘, 위험한 콘텐츠 및 심적 외상에 노출
- 이러한 기본 설정의 위험성에 대한 Epic Games 직원들의 우려 및 아동 괴롭힘에 대한 신고에도 불구하고 Epic Games는 게임 내에서 음성 및 문자 채팅 기능을 옵트인 방식으로 바로 변경하지 않았으며, 채팅 비활성화 도입 이후에도 해당 버튼을 찾기 어렵게 배치

▶ **(다크패턴)** Epic Games는 Fortnite에서 '직관적이지 않고, 비일관적이며, 혼란스러운' 버튼 배치와 싱글 버튼 결제 시스템을 통해 모든 연령대의 사용자가 의도치 않은 게임 내 구매를 하도록 유도

- 이에 따라 사용자들은 버튼 하나만 눌러도 원치 않은 과금이 발생했으며, 구매 버튼이 아이템 미리보기 버튼에 인접하게 배치되었기에 사용자들이 실수로 결제하는 상황이 빈번히 발생
- 또한, 게임 스토어에서 부모의 구매 승인 절차가 부재했기에 아동이 게임 중 쉽게 부모의 신용카드로 무단 구매가 가능했던 정황이 확인되었으며,

- Epic Games는 무단 청구와 관련해 신용카드 회사에 이의를 제기한 사용자들의 계정을 잠금 조치함

(2) 아일랜드 개인정보 감독기관(DPC), Meta에 12억 유로의 과징금 부과

① 개요

▶ DPC는 EU 개인정보보호이사회(EDPB, European Data Protection Board)의 구속력 있는 결정('23.4.13.)을 반영하여 Facebook 소셜미디어 플랫폼 서비스를 제공하는 Meta Platforms Limited(이하 Meta 아일랜드)에 GDPR 위반 혐의로 총 12억 유로의 과징금과 시행명령을 부과('23.5.22.)

- 이는 역대 최대 GDPR 위반 과징금인 '21년 룩셈부르크 개인정보 감독기관이 아마존(Amazon)에 부과한 7억 4,600만 유로를 상회하며 GPDR 위반 최대 과징금액을 갱신

▶ Meta 아일랜드는 맞춤형 광고 및 기타 분석 목적을 위해 EU 사용자의 개인정보를 미국으로 전송했으며, 이 과정에서 EU 외부로의 개인정보 이전을 허용하도록 설계된 메커니즘인 표준계약조항(SCC, Standard Contractual Clauses)[10]에 의존

- '15년 10월, EU 사법재판소(CJEU, Court of Justice of the EU)가 슈렘스 I(Schrems I) 판결을 통해 EU와 미국 간의 개인정보 이전 협정인 세이프하버(Safeharbor)를 무효화 했으며, 이에 DPC는 Meta 아일랜드의 개인정보 역외이전에 대한 조사의 필요성을 인정[11]

- 이후 막스 슈렘스는 Meta 아일랜드가 세이프 하버 이외에도 EU 시민의 정보를 미국으로 전송하는 근거로 의존한 '10년도 SCC의 적법성에 의문을 제기하며 후속 민원을 새로이 제기('15.12.)

- '20년 7월 16일 CJEU는 세이퍼하버를 대체하기 위해 '16년에 새로 채택된 EU-미국 간 국외이전 매커니즘인 프라이버시 쉴드(Privacy Shield) 또한 슈렘스 II 판결을 통해 무효화

  - 동시에 CJEU는 SCC에 대해 합법적인 개인정보 역외이전을 위한 도구로써의 유효성은 인정하는 한편, EU 역외로 이전된 개인정보의 적절한 보호 수준에 대한 입증이 필요하다고 결정

- '20년 8월, DPC는 Meta 아일랜드에 대한 조사에 착수했으며, 조사 결과 Meta의 현 관행이 GDPR을 준수하지 않으므로 개인정보 전송을 중단해야 한다는 결정 초안을 발표

10) 유럽경제지역(EEA) 내 개인정보를 EEA 외부 국가로 적법하게 전송하기 위하여, 정보 수출자(data exporter)와 정보 수입자(data importer)가 체결하는, EC가 채택하고 발간한 표준 계약서 또는 표준 계약 조항으로, '95년 발효된 '개인정보 처리 관련 자연인의 보호 및 정보의 자유로운 이동에 관한 EU 지침(Directive 95/46/EC)을 기반으로 당해에 최초로 작성되었고, '10년 개정되었다가 CJEU의 '슈렘스 II' 판결 이후 '21년 재개정됨

11) 앞서 '13년 6월, 개인정보 보호 시민단체 noyb를 창립한 오스트리아 변호사 막스 슈렘스(Max Schrems)는 유럽 Facebook 사용자 정보를 미국으로 전송하는 Meta 아일랜드의 위법성을 주장하며 DPC에 민원을 제기한 바 있음

- 그러나 Meta 아일랜드는 EU 집행위원회에서 '21년 개정한 SCC에서 요구한 개인정보 이전에 대한 영향평가(TIA, Transfers Impact Assessment) 및 다양한 기술적·조직적 조치들을 도입했기에, 개정 SCC를 기반으로 개인정보를 미국에 전송하는 것은 위법이 아니라 주장

▶ 원스톱숍 메커니즘에 근거하여 동 사안을 DPC로부터 회부받은 EDPB는 '23년 4월 구속력 있는 결정을 채택했으며, 동 결정을 통해 DPC에 두 가지를 요구

- 즉, DPC가 GDPR 위반에 대해 Meta에 과징금을 부과하되, 과징금 산정의 시작 금액을 해당 법적 상한선의 20~100% 사이에서 결정할 것과,

- Meta가 미국 내에서 EEA 사용자의 개인정보를 저장하는 등의 처리 관행을 중단하고, 처리 업무가 GDPR에 부합하도록 조치하게끔 명령을 내릴 것을 결정

▶ EDPB의 구속력 있는 결정을 반영하여 DPC는 Meta에 대해 12억 유로 과징금을 최종적으로 확정했으며, 과징금 부과 이외에도 Meta 아일랜드에 규정 준수를 위해 결정 통보일로부터 5개월 이내에 시정명령을 내림('23.5.)

- Meta는 GDPR 준수를 입증할 수 있을 때까지 향후 미국으로의 모든 개인정보 이전을 중단해야 함

② 주요 위반 사항

▶ **(개인정보 국외이전을 위한 적정 보호장치)** GDPR 제46조에서 규정한 EU 역외 국가로 개인정보를 전송하는 경우 적절한 보호조치를 취할 의무를 위반

- Meta 아일랜드는 Facebook 서비스와 관련해 미국으로 개인정보를 이전하기 위한 법적 근거로 SCC에 의존했지만, SCC가 미국 정보기관의 감시로부터 개인정보를 효과적으로 보호할 수 있다는 점을 입증하지 못했음

- DPC는 Meta 아일랜드가 본질적으로 미국 해외정보감시법(Foreign Intelligence Surveillance Act, 이하 FISA) 제702조의 적용을 받는 기업이며, 미국 정부의 정보 요청에 응해야 한다는 사실이 변하지 않는다는 점에서 SCC 모두 충분한 보호를 보장하지 못한다고 판단

- 따라서 DPC는 Meta 아일랜드가 미국으로의 개인정보 전송 근거로 삼고 있는 SCC 및 추가적인 보호 조치들이 미국 법률에 따른 보호의 부적절성을 보상하기에 충분치 않다고 결론

- 아울러 DPC는 Meta 아일랜드에서 체계적·반복적·대규모로 이루어지는 개인정보 전송에 대해 GDPR 제49조에 명시된 예외조항(예컨대, 계약상의 필요성 또는 공익 목적)을 적용할 수 없다고 판단

(3) 브라질 ANPD, LGPD 위반에 대해 첫 행정처분 부과

① 개요

▶ 브라질 개인정보 감독기관(ANPD)는 '22년 3월, 통신사 Telekall Info Sevices(이하 Telekall)이 DPO를 임명하지 않았으며, 개인정보 수집에 앞서 정보주체의 동의를 얻지 않았다는 혐의에 대한 조사에 착수

- '21년 2월 28일, 브라질의 '20년 지방 선거와 관련하여 Telekall이 메시징 앱을 통해 우바투바(상파울루) 지역 유권자의 연락처 목록을 제공했다는 민원이 제기

▶ '23년 7월, ANPD는 Telekall에 대해 경고 조치 및 총 1만 4,400헤알(약 2,938 달러)의 단순 과징금을 부과

- 이는 ▲브라질 개인정보보호법(LGPD) 제41조 위반에 대한 경고 ▲LGPD 제7조 위반에 대한 7,200헤알(약 1,469달러) 과징금 ▲ANPD의 감독 절차 및 행정 제재 절차 규정(CD/ANPD No.1/2021) 제5조 위반에 대한 7,200헤알 과징금 등으로 구성
- 한편, 동 행정처분 결정은 ANPD가 운영을 개시한 이래로 LGPD 위반에 대해 최초로 제재 절차를 진행하여 과징금을 처분한 사례임

② 주요 위반 사항

▶ **(적법한 처리 근거)** ANPD는 Telekall이 공개적인 데이터를 2차 목적으로 사용했으며, 해당 처리에 대한 적절한 법적 근거가 없음을 확인

- Telekall은 정치인들이 대량의 선거자료 배포 메시지를 전송할 수 있도록 적법한 근거 없이 유권자들의 WhatsApp 연락처를 제공한 것으로 확인
- 이러한 처리 활동에는 명백히 경제적 이득을 취하려는 의도가 있었기에, 개인정보 처리에 대한 모든 법적 근거를 나열한 LGPD 제7조를 위반한 것으로 간주
- 특히 ANPD는 공개적으로 이용가능한 개인정보의 처리 활동과 관련해 투명성의 필요성을 강조
- 동 사건의 경우 컨트롤러인 Telekall이 정보주체에게 본인의 개인정보가 어떻게 처리되고 있는지 투명하게 공개하지 않았기에, ANPD는 정보주체가 원래 개인정보를 공개했던 목적 이외의 다른 목적을 위해 컨트롤러가 정당한 이익을 개인정보 처리의 법적 근거로 지정할 가능성을 거부

▶ **(DPO 임명)** 또한, Telekall은 개인정보 처리와 관련하여 ANPD와의 소통을 담당할 개인정보보호책임자(DPO, Data Protection Officer)를 적시에 임명하지 않아, LGPD 제41조를 위반

▶ **(ANPD 협조)** ANPD는 Telekall이 해당 사건과 관련해 제출할 것을 요청받은 문서 및 정보를 최초 요청에 따라 즉시 제공하지 않았으며, ANPD의 공식 요청에 소극적으로 임한 점을 확인

- 이는 조사 업무를 수행하는 ANPD가 요구하는 대로 컨트롤러가 관련 문서 및 정보 사본을 ANPD에 제공하도록 규정한 결의안(CD/ANPD No.1/2021) 제5조 위반에 해당
- 이와 같은 의무사항의 미준수는 ANPD의 조사 활동을 방해하는 것으로 간주되어 '심각한 위반'으로 구분

3. 평가 및 시사점

▶ Epic Games와 FTC의 이번 합의는 아동 보호의 중요성을 강조함과 동시에 다크패턴 사용으로 인한 잠재적 불이익에 대한 경각심을 업계 전반에 일깨워주는 사례로 작용

- 13세 미만 아동을 대상으로 하는 상업용 웹사이트는 사용자로부터 개인정보를 수집하기 전 확인 가능한 부모의 동의를 얻어야 하는 의무를 포함해 COPPA 요건을 엄격히 준수할 필요성이 두드러졌으며,
- 이를 준수하지 않을 경우, 각 위반에 대한 과징금을 비롯해 불법 수집 정보 삭제 명령, 감사·감독 명령, 평판 훼손 및 기타 법적·비즈니스상의 불이익을 받을 위험이 있음
- 특히 FTC는 개인정보 정보 영역의 다크패턴 단속까지 감독 활동 범위를 확대하고자 하는 움직임을 보이고 있으며, 이러한 동향은 미국 주 정부 차원에서도 비슷하게 전개되고 있음
- 대표적으로 캘리포니아주는 미국에서 다크패턴의 사용을 금지하는 소비자 개인정보 보호법을 제정한 미국 최초의 주이며, 콜로라도주를 비롯한 다른 주 또한 개인정보 관련 다크패턴 규제를 위한 입법 활동을 전개하고 있음
- 이에 따라 기업들은 콘텐츠가 표시되는 방식, 기본 설정 구현, 옵트아웃 옵션 접근 방식 및 기타 사용자 인터페이스 디자인 구현에 있어 더욱 신중해야 하며,
- 콘텐츠 출시에 앞서 다크패턴으로 간주할 수 있는 불법적인 디자인 패턴을 식별하고 적절한 실사 및 리스크 관리가 중요해질 전망

▶ 아일랜드 DPC의 Meta 아일랜드에 대한 과징금 부과 사례는 GDPR 요건을 준수하는 개인정보 역외이전 메커니즘의 필요성에 대한 인식을 제고

- 동 결정은 국경을 넘나드는 개인정보 전송을 위해 여러 기업이 널리 사용하고 있는 EU 집행위원회 승인 SCC의 적절성에 의문을 제기한다는 점에서 중요성을 시사

- EDPB의 구속력 있는 결정을 반영한 DPC 결정은 '21년 개정된 SCC조차 모든 상황에서 절대적으로 신뢰할 수 없다는 점을 분명히 하고 있음
- 따라서 EU의 SCC에 의존하여 개인정보를 전송하고자 하는 기업은 이에 안주하지 않고, DPC의 조사 결과를 참고하여 개인정보 이전 위험평가를 제대로 수행하고 있는지, 그리고 적절한 보완 조치를 채택했는지 철저히 점검하는 것이 중요

▶ 브라질 ANPD가 Telekall에 대해 내린 과징금 결정은 LGPD 미준수로 인해 ANPD가 제재를 가한 첫 번째 사례라는 점에서 매우 중요한 결정으로 평가

- 이는 향후 ANPD가 다양한 규모의 기업을 포함하여 유사한 위반 사례에 대해 어떻게 처리할 것인지에 대한 선례로 작용할 전망

Reference

1. Clearly Gottlieb, Key Takeaway's from the Irish Data Protection Commission's decision on Meta Data Transfers, 2023.8.7.
2. CMS GDPR Enforcement Tracker, Fines Statistics, https://www.enforcementtracker.com/?insights
3. CMS Law, Enforcement Tracker Report 2022/2023
4. Dataguidance, Enforcement Dashboard, https://preview.dataguidance.com/enforcement-dashboard?check_logged_in=1
5. Fieldfisher, Epic Games / FTC $520M Settlement – what does this mean for Children's privacy in Europe?, 2023.1.23.
6. FTC, FTC Finalizes Order Requiring Fortnite maker Epic Games to Pay $245 Million for Tricking Users into Making Unwanted Charges, 2023.3.14.
7. Global Compliance News, Brazil: First sanction for non-compliance with the General Data Protection Law, 2023.7.19.
8. Macfarlanes, Meta handed the largest fine in GDPR history for breach of international transfer provisions, 2023.6.1.
9. Privacy Rules, Brazilian ANPD first fine for violation of the LGPD, 2023.7.13.
10. 뉴시스, '29만건 개인정보 유출' LGU+ 과징금 68억원 제재(종합), 2023.7.12.
11. 신아일보, '개인정보위 과징금 소송' 대형 로펌 가세...'다윗-골리앗 싸움', 2023.10.22.

2023년 국내외 개인정보 이슈 점검과 2024년 주요 이슈 전망

[목 차]

1. 개요

▶ '23년은 생성형 AI*의 등장에 따른 사회적 파급력으로 인해 생성형 AI와 연관된 개인정보보호 이슈가 급부상한 한 해로 기록

* 대규모의 데이터 세트를 학습한 딥러닝 모델을 활용하여 이용자의 요구에 따라 결과값을 생성해 내는 인공지능(AI) 기술

- 생성형 AI는 대규모 데이터 세트를 바탕으로 학습을 수행하기 때문에, 학습 과정에서 데이터 세트에 포함되어 있는 무수한 개인정보를 함께 학습

- 이에 따라 AI가 출력하는 결과값에 개인과 관련한 다양한 정보가 포함될 위험성이 상존하고 있으며, 이는 학습 데이터에 따라 성차별, 인종차별 등과 같은 AI의 윤리적 문제를 비롯해 정보주체에 대한 개인정보 침해 문제를 구성

▶ 그밖에 유럽연합(EU) 일반 개인정보보호법(EU GDPR)이 '18년 이후 약 5년간 시행되면서 정착기에 접어듦에 따라, 각국의 개인정보보보호 관련 법제도 또한 다음 단계로 발전하는 경향을 보임

- 예컨대, 포괄적인 개인정보보호법 이외에도 아동 개인정보, 민감한 개인정보 등과 같이 구체적인 영역에서 더욱 특화된 법률 및 제도가 도입되거나 추진

▶ 이하에서는 '23년 한 해 개인정보보호 동향 모니터링을 토대로 개인정보보호 관련 이슈를 점검하고, '24년에 주목받게 될 주요 이슈를 조망하기로 함

2. '23년 국내외 개인정보보호 이슈 점검

(1) 생성형 AI 대두와 개인정보보호 관련 대응

① 배경

▶ '22년 11월 오픈AI(OpenAI)의 챗GPT(ChatGPT) 등장과 함께 생성형 AI가 전 세계적으로 빠르게 확산

- 챗GPT의 돌풍 이후 빅테크도 생성형 AI 시장 경쟁에 합류했으며, 마이크로소프트의 빙챗(Bing Chat), 구글의 바드(Bard) 등이 연달아 출시

▶ 생성형 AI의 확산과 관련해 무분별한 개인정보 수집 및 처리 등이 문제로 지적되면서 주요국은 거버넌스, 법 제정, 집행 등 다양한 방식으로 대응에 나섬

② 국내 동향

▶ 개인정보보호위원회(이하 개인정보위)는 '23년 7월, 챗GPT 운영사인 오픈AI에 대해 정보 유출 신고의무 미준수를 이유로 과태료 360만 원을 부과하고 재발 방지 대책 수립 등 관행 개선을 위한 권고를 결정[12)]

▶ 그밖에, 개인정보위는 생성형 AI의 등장을 비롯해 변화하는 AI 시장에 능동적으로 대응하고 AI 사업자의 법률 준수 등을 지원하고자 AI를 전담하는 'AI 프라이버시팀'을 신설[13)]

12) 지디넷코리아, 오픈AI, 국내 첫 개인정보 보호 위반 제재, 2023.7.27.
13) 전자신문, 개인정보위, AI 시대 개인정보 보호 정책 발표…전담팀 신설, 202.8.3.

- AI 프라이버시팀은 AI 사업자의 법률 위반을 미연에 방지하기 위해 개인정보보호 원칙에 대한 유권해석이나 사안별로 개인정보 처리의 적법성·안전성 등 법령해석을 지원

③ 해외 동향

▶ EU는 '23년 12월 AI 법(안)(AI Act) 제정을 위한 EU 이사회 의장단과 유럽의회 협상단 간 합의에 잠정 도달

- 동 법안은 EU집행위원회가 '21년 4월에 최초 제안한 후 '21년 말 챗GPT 돌풍과 함께 안건 심의가 가속화
- 세계 최초의 포괄적인 AI 규제법이 될 것으로 평가되는 AI 법(안)은 법률을 위반하는 기업에 대해 최대 3,500만 유로 또는 연간 세계 매출의 7%에 해당하는 높은 과징금을 규정
- 현 법안에서는 생성형 AI를 직접적으로 언급하지는 않고 있으나 AI를 위험 수준에 따라 유형별로 구분하고 있어 생성형 AI의 특성에 따라 해당 범주별 규제를 적용받게 됨

▶ 그밖에 유럽 각국에서도 대표적 생성형 AI인 챗GPT에 대한 개인정보보호 관련 규제 및 집행 추진

- 이탈리아 개인정보 감독기관은 챗GPT의 운영사 오픈AI의 개인정보 불법 수집을 근거로 개인정보 수집 행위에 대한 개선이 이루어질 때까지 이탈리아 이용자의 개인정보 수집 중단을 명령하며 역내 서비스를 일시 차단[14] ('23.3.)
- 폴란드 개인정보 감독기관은 챗GPT의 GDPR 위반에 관한 다수의 민원 및 불만사항을 접수하고 '23년 9월 오픈AI에 대한 개인정보보호 위반 여부에 대한 조사에 착수[15]

▶ 일본 정부는 생성형 AI에 대한 개인정보 수집 관행을 문제 삼아 경고를 내리거나 생성형 AI가 초래할 수 있는 위험의 경감을 위한 제도 신설을 검토

- 일본 개인정보 감독기관은 '23년 6월 OpenAI에 대해 개인의 동의없이 민감정보를 수집하지 말라고 경고하고 이를 준수하지 않을 경우 추가조치를 취할 수 있음을 시사[16]
- 그밖에 일본 정부는 '23년 11월 열린 'AI 전략회의'에서 생성형 AI 사업자 등과 관련한 위험 경감책의 일환으로서 제3자 인증제도나 외부 감사 도입 등을 검토하고 있음을 밝힘[17]

▶ 미국은 '23년 10월 미국 시민의 안전 보장과 개인정보보호, 형평성 증진, 혁신 및 경쟁 촉진을 위해 안전하고 신뢰할 수 있는 AI에 관한 행정명령을 발령

14) The Verge, Italian regulators order ChatGPT ban over alleged violation of data privacy laws, 2023.3.31.
15) TechCrunch, Poland opens privacy probe of ChatGPT following GDPR complaint, 2023.9.21.
16) Reuters, Japan privacy watchdog warns ChatGPT-maker OpenAI on user data, 2023.6.2.
17) 読売新聞, 生成ＡＩ開発、第三者が認証する仕組み創設検討…リスク軽減へ規制強化, 2023.11.7.

- 동 행정명령은 영향력이 큰 생성형 AI 모델을 개발하는 기업으로 하여금 정부에 세부사항을 알리고 테스트 결과를 공유하도록 의무화하는 내용을 포함[18)]

▶ 생성형 AI는 훈련을 위해 대규모의 데이터 세트에 의존할 수밖에 없는데, 개인정보보호 강화기술은 생성형 AI의 규범 준수에도 기여할 것으로 예상

- 예컨대, 생성형 AI가 학습과정에서 개인정보 또는 민감정보가 포함된 데이터 노이즈를 무작위로 주입받더라도 개인정보보호 강화기술을 통해 결과값에서 개인정보를 추론할 수 없게 훈련될 수 있음

- 이 경우 생성형 AI가 출력한 결과값에서도 개인정보의 익명성이 유지됨으로써 개인정보를 포함한 데이터 세트로도 적법성을 유지한 채 훈련 수행이 가능

(2) 마이데이터 도입 확대

① 배경

▶ '22년 1월에 마이데이터(본인신용정보관리업)* 서비스가 본격 시행된 후, 국내에서는 국민이 주도하는 마이데이터 생태계 구축에 박차를 가함

* 개인신용정보 전송요구권의 행사를 기반으로 분산되어 있는 신용정보를 통합하여 개인에게 제공하는 행위를 영업으로 하는 것을 지칭(신용정보법 제2조제9호의2)

- 우리나라 정부는 데이터 활용보다 개인정보 보호에 주력하는 양상을 보였으나, 데이터3법 개정을 기점으로 데이터 자기결정권을 기반한 신용정보 생태계를 구현하는 마이데이터 사업이 국내에서 본격화

② 국내 동향

▶ '23년 8월, 정부는 관계부처 합동 '국가 마이데이터 혁신 추진전략'을 발표하여 마이데이터 제도에 대한 종합적인 청사진을 제시

- 개인정보위는 8개 부처 인력이 협력해 개인정보 전송 요구권 행사를 위한 법제도 세부기준 확립, 기술 지원을 위한 온라인 플랫폼 구축·운영, 데이터 표준화 등 마이데이터 핵심 인프라 구축을 담당할 '범정부 마이데이터 추진단'을 구성('23.7.)

- 개인정보위의 주도하에 '23년 9월 출범한 민·관 합동 '범정부 마이데이터 협의회'는 '24년까지 관련 제도 설계, 선도 프로젝트 발굴, 부처간 이해관계 조정 등 정책 방향을 논의하고 쟁점 사항을 협의 및 조정할 계획

18) Harvard Business Review, 3 Obstacles to Regulating Generative AI, 2023.10.31.

▶ 정부는 산업별 마이데이터 고도화 추진을 위해 금융업계에 마이데이터 제도를 우선 적용했으며, '23년 하반기부터는 금융업계에 이어 의료·통신 마이데이터를 구현하기 위한 논의가 본격화

- '23년 8월 기준 금융 마이데이터 사업자 수는 전년 동월 대비 약 20% 증가한 246개로 집계되었으며, 이는 마이데이터 사업에 금융기관뿐만 아니라 핀테크 업체, 통신사 등 여러 분야의 기업들이 참여한 결과임
- 마이데이터 제도 도입 이후 고객의 전체 금융자산 연결 속도는 20초('23년 상반기 기준)로 단축되었으며, 제도 시행 전(평균 30분)에 비해 정보 수집 속도가 약 90배가 증가한 수치를 보임
- 금융위원회는 지속가능한 마이데이터 산업 기반을 구축하고자 신용정보업감독규정 개정을 추진하여 정보전송비용에 대한 과금 기준 및 과금 산정 절차를 구체화'('23.12.)
- 한편, 현재 국회에서 의료 마이데이터의 근거가 되는 입법적 논의가 이루어지고 있으며, 대표적으로 '디지털 헬스케어 및 보건의료 분야 개인정보보호 및 활용 촉진에 관한 법률안' 및 '디지털 헬스케어 및 보건의료데이터 활용에 관한 법률안'이 발의되어 있음

(3) 개인정보보호 강화 기술(PET)

① 배경

▶ 개인정보보호 강화기술(Privacy Enhancing Technology, 이하 PET)은 개인정보 보안을 극대화함과 동시에 개인정보 처리자의 개인정보 이용을 최소화함으로써 법률에서 요구하는 개인정보보호 요건을 갖춘 채 개인정보를 처리하는 기술을 의미

- 해당 기술을 통해 개인정보 침해 위험을 최소화할 수 있으며, 개인정보에 직접적으로 접근하지 않고서 개인정보를 활용할 수 있다는 장점이 존재
- 최근 PET 활용에 대한 정책기관의 요구가 증가하고 있으며, 개인정보 보호 규제 강화에 따라 국내외 기업에서 사용자 보안 및 개인정보 보호 기능을 강화하는 양상을 보임

② 국내 동향

▶ 개인정보위는 '22년~'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 있음

▶ 또한 개인정보위는 '23년 8월 공개한 '인공지능 시대 안전한 개인정보 활용 정책방향'을 통해 AI 학습 단계에서 활용목적 및 처리환경에 적합한 PET를 적극 활용할 것을 권고

- PET 적용이 모호하거나 검증이 필요한 경우, 보안성과 안전성이 확보된 공간에서 기술 개발 및 실증을 할 수 있도록 후속 조치를 마련키로 함

▶ '23년 10월 개인정보위는 '개인정보 안심 구역' 시범운영기관 지정 공모에 착수했으며, 이로써 실제 연구 개발이 어려웠던 PET에 대한 실증사업을 추진

③ 해외 동향

▶ 개인정보 감독기관들과 국제기구들은 컨트롤러들의 GDPR 준수를 지원하기 위해 PET의 활용을 권장하는 추세

- 영국 개인정보 감독기관(ICO)은 '23년 6월, PET에 대한 온라인 가이드라인을 공개했으며, ▲PET가 UK GDPR 규정 준수를 촉진하는 방법을 설명하고 ▲현재 가용할 수 있는 8가지 유형의 PET의 장단점을 소개

- ICO 가이드라인에서 소개한 PET의 대표적인 예는 합성 데이터(synthetic data)로, 이는 개인정보가 포함된 대규모 데이터 세트에 액세스해야 하는 작업에 유용

- 또한 경제협력개발기구(OECD, Organization for Economic Co-operation and Development)는 PET 관련 보고서 발행을 통해 다양한 PET 유형의 효과 및 가치를 소개함과 동시에 PET에 대한 현행 규제 및 정책 접근 방식을 설명

(4) 개인영상정보 보호 및 활용

① 배경

▶ 공공 안전 및 범죄 예방의 목적으로 CCTV, 블랙박스, 드론, 자율주행차 등 각종 영상정보처리기기의 운영 규모는 매년 국내외에서 꾸준히 증가*하고 있음

* 개인정보위는 '22년 말 기준 우리나라에 설치된 CCTV 개수가 약 1,960만 대에 달한다는 조사 결과를 공개

- 최근에는 AI를 활용한 영상분석 기능을 탑재한 지능형 CCTV의 도입 또한 활발히 진행되고 있는 양상을 보임

- 그러나 동시에 영상정보처리기기 촬영 영상의 대량 유출 및 무단 배포 사건 발생으로 인해 개인정보 침해의 우려가 증폭되며 개인정보 보호 강화를 위한 법제도 마련의 필요성이 주목받음

② 국내 동향

▶ '23년 3월, 윤주경 의원 등 15인은 '영상정보 처리기기의 설치·관리 및 개인영상정보의 보호 등에 관한 법률안'을 발의한 바 있음

- 동 법안은 ▲영상정보처리기기의 설치, 운용 및 관리 ▲관제시설 종사자의 자격 및 교육 ▲개인영상정보의 활용, 제공 및 보호조치 등에 대한 기준과 절차를 구체적으로 명시함으로써, 영상정보의 안전한 활용을 촉진함과 동시에 영상정보처리기기로 인해 침해받을 위험이 있는 국민의 기본권을 보호하고자 함

▶ 또한 보건복지부는 의료법 제38조의2(수술실 내 폐쇄회로 텔레비전의 설치·운영) 규정의 시행('23.9.)에 따라 '수술실 폐쇄회로 텔레비전 설치·운영 기준(가이드라인)'을 배포

- 해당 가이드라인을 통해 복지부는 ▲수술실의 개념을 회복실, 치료실, 임상검사실과 구분하고 ▲환자가 의식이 없는 상태에서는 CCTV를 설치해야 함을 명확히 하며 ▲기본적으로 수술을 받는 환자나 보호자의 요청 없이 의료기관이 임의로 수술 장면을 촬영할 수 없다는 법 해석을 제시

③ 해외 동향

▶ '23년 6월, ICO는 중소기업을 위한 CCTV 설치·운영 권고사항을 발표한 바 있으며, 덴마크 개인정보 감독기관 또한 민간기업을 대상으로 CCTV 감시에 대한 지침을 공개한 바 있음

▶ 한편, 중국산 CCTV에 백도어(Backdoor)*가 설치되어 있어 개인정보 및 프라이버시 침해 우려가 세계적으로 확산하였으며, 미국·영국·호주 등 영미권 국가들에서는 이러한 중국산 CCTV에 대한 보이콧 동향이 포착

* 기기를 원격에서 수리하거나 관리하기 위해 시스템 설계자나 관리자가 남겨둔 우회 접근 방식

(5) 개인정보 역외이전 및 국가 간 교류

① 배경

▶ 비즈니스의 다양화 및 각 기업의 자유로운 데이터 흐름에 대한 요구 증가로 인해 높은 수준의 개인정보보호 요건을 갖춘 국가 간 개인정보 및 데이터의 용이한 상호 교류 문제가 대두

- 특정 국가의 기업이 마케팅 전략을 새롭게 수립하기 위해 해당 분야의 전문성을 가진 타 국가 소재 기업에 자사가 보유한 개인정보를 전송하여 데이터 분석을 의뢰하고자 할 경우에도, 개인정보 국외이전 요건을 갖추기 위해 수많은 절차를 거쳐야 하는 실정

- 반대로, 일정 수준 이상의 개인정보보호 요건을 갖추지 못한 국가에 소재한 소셜미디어 기업이 타국 이용자의 개인정보를 과도하게 처리한다고 여겨질 경우, 해당 소셜미디어의 자국 내 서비스 중단 조치를 취하는 경우도 존재

② 국내 동향

▶ 우리나라는 EU집행위원회(European Commission)('21.12.) 및 영국 디지털문화미디어스포츠부(Department for Digital Culture, Media & Sport)('22.12.)로부터 국외이전에 대한 적정성 결정을 이끌어 냄

- 적정성 결정은 타국의 개인정보보호 수준을 평가하여 추가적인 인증이나 절차 없이 전송할 수 있도록 승인하는 일종의 화이트리스트 제도로, EU 및 영국 등이 해당 제도를 운영
- 이를 통해 EU 회원국 및 영국 내에 존재하는 개인정보가 우리나라로 전송되는 과정이 간소화되어, 해당 지역 및 국가로부터 대한민국으로의 비교적 자유로운 데이터 흐름이 가능해진 상황

▶ 반대로 개인정보보호위원회(개인정보위) 또한 EU 등으로부터 개인정보 이전에 대한 강력한 문호 개방을 요구받았으며, '23년 10월 개인정보 국외이전 요건을 다양화하는 '개인정보 국외 이전 운영 등에 관한 규정'을 제정 및 시행한다고 발표[19)]

- 해당 규정은 '23년 9월부터 시행에 돌입한 개인정보 보호법 및 동 시행령에서 위임한 국외이전에 관해 상세한 내용을 담고 있는데, 정보주체의 동의 이외에도 국내 개인정보를 역외로 이전할 수 있는 다양한 근거를 마련하는 취지
- 대표적으로 동 규정에서는 개인정보 국외이전 관련 평가를 담당하는 국외이전전문위원회의 구성 및 운영에 관한 내용을 담고 있음
- 국외이전전문위원회가 개인정보 이전대상국의 보호 수준 평가를 수행한 후 개인정보위가 개인정보 국외이전 대상국으로 인정할 경우, 해당 국가 기업이 우리나라 역내에서 수집한 개인정보를 자국으로 자유롭게 이전할 수 있게 됨

③ 해외 동향

▶ EU와 미국은 EU로부터 미국으로의 개인정보 이전에 관한 기존 무효화된 법적 근거를 새로이 정립

- EU집행위원회는 EU로부터 미국으로의 자유로운 데이터 흐름을 위한 자체적 인증 수단인 'EU-미국 데이터 프라이버시 프레임워크(EU-US Data Privacy Framework)'에 대한 적정성 결정을 채택 ('23.7.10.)
- 해당 적정성 결정은 EU사법재판소가 양자 간 기존 인증 수단이었던 'EU-미국 프라이버시 쉴드(Privacy Shield)' 협약을 무효화하는 결정(Schrems II)을 내린 후 상호 간 개인정보 역외이전 문제를 다시금 회복하려는 조치

19) 보안뉴스, 개인정보위, '개인정보 국외 이전 운영 등에 관한 규정' 10월 16일 제정·시행, 2023.10.12.

- 해당 프레임워크를 바탕으로 EU 역내의 개인정보를 미국으로 이전하고자 할 경우, 표준계약조항 또는 구속력 있는 기업 규칙 등과 같은 다른 이전 메커니즘에 의존하거나 이전 영향 평가(Transfer Impact Assessment)를 수행하지 않고서도 미국으로의 데이터 전송이 가능해짐

▶ 중국 정부는 개인정보 국외이전 표준계약규정(个人信息出境标准合同办法)을 공표하고 '23년 6월 1일부터 시행에 돌입

- 동 규정은 중국 개인정보보호법 제38조에서 규정하고 있는 중국 내 개인정보의 역외 이전과 관련, 그 중 하나인 표준계약에 의한 방식의 상세 내용을 기술

- 구체적으로 ▲개인정보 국외이전 시 표준계약을 체결할 수 있는 구체적 요건 ▲중국 역내 개인정보처리자의 개인정보보호 영향평가 실시 의무 ▲표준계약 발효 후 주무부서 신고 의무 등을 포함

(6) 개인정보 보호법령 제정·개정

① 배경

▶ '23년은 EU GDPR의 시행 5주년을 맞이한 해로, 전 세계적으로 개인정보 보호법 제정 및 개정 움직임이 활발히 진행

▶ 우리나라는 국회가 '20년에 데이터3법 개정으로 개인정보 보호법을 대대적으로 개편한 데 이어, '23년 2월 27일에 개인정보 보호법을 대폭 개정하는 새로운 법안을 가결

- 이러한 개정안을 반영한 개정 개인정보 보호법은 '23년 9월 15일부터 시행되었으며, 개인정보 전송요구권 및 자동화된 의사결정에 대한 이의제기권 등 일부 조항은 대통령 공포일로부터 1~2년 후에 시행 예정

② 국내 동향

▶ 9월 15일에 시행된 개인정보 보호법 개정법은 ▲정보주체의 권익 보호 ▲온·오프라인 이중 규제 등 개선 ▲공공기관 안전성 강화 ▲글로벌 스탠다드 등 중심으로 정비

- 이러한 개정 사항과 관련해 개인정보위는 대중의 이해를 돕기 위해 '개인정보 보호법 및 시행령 개정 안내서' 초안을 공개('23.9.27.)

③ 해외 동향

▶ 미국은 '23년에 가장 많은 개인정보 보호법을 제정한 국가이며, 이는 현재까지 연방 차원의 개인정보 보호법이 마련되지 않아 주(州) 단위로 법을 제정하고 있기 때문

- '23년 한 해 동안 총 7개 주(▲유타주 ▲플로리다주 ▲몬태나주 ▲아이오와주 ▲텍사스주 ▲델라웨어주 ▲테네시주 ▲인디애나주)에서 포괄적인 개인정보보호법이 제정되었으며, 4개 주(▲버지니아주 ▲콜로라도주 ▲코네티컷주 ▲유타주)의 개인정보보호법이 시행

- 한편 CPRA(캘리포니아 소비자 개인정보 보호법)를 통해 개정된 CCPA(캘리포니아 개인정보 보호법)는 본래 '23년 7월 시행 예정이었으나, 새크라멘토 상급 법원은 시행일을 '24년 3월로 연기 판결('23.6.)

▶ 인도에서는 최초의 포괄적인 개인정보 보호법(DPDPA 2023)이 제정('23.8.11.)되었으며, 사우디아라비아는 기존 개인정보 보호법(PDPL)을 개정('23.3.21.)

- 이 외에도 호주와 영국에서 현행 개인정보 보호법을 대폭 개정하기 위한 논의가 본격적으로 진행

(7) 플랫폼 규제

① 배경

▶ 국내외적으로 온라인 플랫폼의 활성화는 소비 행태의 디지털 전환을 이끌어 낸 한편, 개인정보 보호 침해, 반독점 논란 등의 역기능을 불러일으키는 결과를 초래

- 이와 관련해 EU, 미국 등은 플랫폼 규제를 강화하고자 반독점 패키지 법안, 디지털 시장법(DMA, Digital Markets Act) 등을 도입하였으며, 국내에서는 개인정보 보호를 강화함과 동시에 산업혁신과 역동성을 저해하지 않는 플랫폼 자율규제를 국정 과제로 추진

② 국내 동향

▶ '23년 11월, 플랫폼 자율규제의 법적 목적 및 근거를 구체적으로 명시한 '전기통신사업법' 개정안이 의결

- 동 개정안은 자율 규제 업무 수행 목적으로 ▲민간에서의 건전한 거래 질서 확립 ▲혁신 촉진 ▲이용자 보호 및 상행협력 등을 명시했으며, 효율적인 자율규제 수행을 위해 자율기구 설치 및 운영의 근거를 마련

▶ 네이버는 자율 규제 역량 강화를 위해 이용자 보호·자율규제 위원회를 출범하였으며, 카카오는 AI 윤리 정책을 강화한 AI 체크리스트를 수립하는 등 기술 윤리 거버넌스 체계를 고도화

③ 해외 동향

▶ 한편 미국에서는 최근 상승세를 보이고 있는 TikTok 등 중국 플랫폼에 대한 견제를 목적으로 올해 의회에 발의되었던 빅테크 기업 규제 법안 6개 중 5건을 폐기

▶ 미국의 이러한 자국 기업 보호 움직임은 Google, Amazon, Apple, Meta 등 빅테크에 대한 규제를 강화하고자 하는 EU의 움직임과 상반됨

- EU에서는 온라인 플랫폼을 적용 대상으로 하는 디지털 서비스법(DSA, Digital Services Act)가 두 단계에 걸쳐 시행되었으며,
- 구체적으로는 ▲'22년 11월에는 초대형 온라인 플랫폼(VLOP, Very Large Online Platforms)를 제외한 의무가 발효 ▲'23년 8월 25일에는 최소 4,500만 명의 활성 사용자를 보유한 VLOP에 대한 DSA 의무가 발효

3. '24년 개인정보보호 분야 부상 이슈 점검

(1) ESG 경영과 개인정보 보호·데이터 보안

▶ ESG(환경·사회·지배구조)[20] 경영이 기업의 미래 경쟁력을 결정하는 중요한 기준으로 대두되고 있는 가운데, '24년에는 개인정보 보호와 기업의 ESG 성과 간의 상관관계가 더욱 주목받을 전망

▶ 그동안 ESG와 전형적으로 연관되는 이슈는 탄소 배출량 감소, 기업 윤리, 인적자본 개발 등이었으나, 최근 더 많은 기업이 개인정보 보호를 기업의 사회적 책임과 지속가능성에 직접적인 영향을 미치는 요소로 인식

- 기업의 개인정보 침해는 막대한 금전적 과징금을 초래할 뿐 아니라 소비자의 신뢰와 기업 평판을 잃는 요인이 되며, 잃었던 신뢰와 평판은 빠르게 회복하기 어려움
- 최근 대규모 개인정보 유출 사고의 연이은 발생으로 인해 대중의 개인정보 보안 인식이 제고되어, 사회적 책임을 다하는 영리 기업에 대한 대중의 요구가 증가하는 추세

▶ 투자자들이 개인정보 보호를 기업의 핵심 ESG 성과 지표로 취급하는 추세가 강화될 것으로 예상되며, ESG 경영을 추구하는 기업은 데이터와 기술을 책임감 있게 사용하여 지속가능한 가치를 창출하는 것이 필요

20) ESG 프레임워크는 기업이 사회와 환경에 미치는 경제적, 환경적, 사회적 영향을 식별, 평가 및 통합하고자 기업의 비재무적 성과를 측정하는 지표. ▲Environment(환경) 기준은 기업이 자연환경에 미치는 영향을 평가 ▲Society (사회) 기준은 노동 관행, 인권, 지역사회 참여 등 기업이 사회에 미치는 영향을 조사 ▲Governance(지배구조) 기준은 기업의 리더십, 내부 통제 및 전반적인 윤리적 관행을 평가.

- 이에 따라 초기 단계부터 개인정보 보호를 염두에 두고 제품, 서비스 및 시스템을 설계하는 '개인정보 보호 중심 설계(Privacy by Design)'의 중요성이 강조
- 또한 감독기관들의 규제 압력에 따라 개인정보를 취급하는 기업들을 리스크를 선제적으로 파악하고 침해사고 대응을 위한 내부 정책과 절차를 적극적으로 마련해야 할 것
- 더 많은 기업이 데이터 분석, 마케팅, 클라우드 서비스 등의 분야에서 타사와의 개인정보 공유 관행에 대한 감독기관 조사에 대응할 수 있는 엄격한 거버넌스 체계를 갖출 것으로 평가

(2) 개인정보 유출 위험 완화 AI 기술[21)]

▶ 개인정보 보호를 위협하는 요소는 계속 증가할 것으로 예상되며, 해커와 같은 인간뿐만 아니라 개인정보가 포함된 자료를 무분별하게 학습하는 AI 등의 기술도 모두 포함

▶ AI는 대규모 데이터 세트를 신속 분석함으로써 패턴을 감지하고 학습을 통해 유사한 새로운 상황에도 활용될 수 있어 개인정보보호 위험을 효과적으로 식별하고 완화하는 데 유용한 기술로 각광

- 즉, AI의 개인정보보호 위협 시도를 AI로써 방어하는 것으로, 이는 ▲인간이 인지할 수 없는 영역의 위험 감지 역량 ▲인간을 능가하는 처리 속도 등을 보유한 AI 기술만의 장점에 해당
- 따라서 기업이 개인정보 유출 위험을 최소화하기 위해 어떠한 방식으로 AI를 학습시키고 AI 기술을 활용해야 하는지가 향후 기업 리스크의 효율적 관리 측면에서 중요 이슈로 조명될 가능성이 큼

(3) 자동차 산업의 개인정보 과다 수집[22)]

▶ 웹브라우저 파이어폭스 운영사로 유명한 모질라 재단(Mozilla Foundation)은 최근 총 25개 브랜드의 자동차사를 대상으로 한 개인정보 수집에 관한 조사 결과를 발표

- 조사 대상 브랜드 중 92%는 운전자에게 자신의 개인정보에 대한 통제권을 제공하지 않았으며, 84%는 해당 데이터를 외부의 제3자와 공유하는 것으로 나타남
- 또한, 이들 모두 모질라 재단이 설정한 최소 개인정보보호 기준을 충족하지 못했으며, 운전자로부터 필요 이상으로 많은 개인정보를 수집하는 것으로 드러남

21) BigID, 10 Data Privacy Predictions for 2024 & Beyond, 2023.12.7.
22) The Verge, 'Modern cars are a privacy nightmare,' the worst Mozilla's seen, 2023.9.6.

- 수집되는 데이터는 의료 개인정보에서부터 운전자가 차량을 활용하는 방식, 예컨대 주행속도, 운전 장소, 청취 음악 등에 이르기까지 다양

- 그밖에, 개인정보 암호화 및 도난 방지에 관해서도 모질라 재단의 최소 보안 표준을 충족한 곳은 한 군데도 없었다고 지적

▶ 자동차 회사의 개인정보 과다 수집 및 부적절한 처리 활동이 문제가 되는 가운데, 향후 각국 개인정보 감독기관이 감독 과정에서 어떠한 쟁점을 주로 거론할 것인지에 대해 귀추가 주목

- ▲정보주체인 운전자의 개인정보보호 권리에 대한 제어권 회복 여부 ▲개인정보의 제3자 무단 제공에 대한 동의 획득 여부 ▲과도한 개인정보 처리에 관한 정보 제공 이행 여부 ▲개인정보 보안을 위한 기술적 조치를 마련했는지 여부 등이 대표적인 예시가 될 것으로 관측

(4) 서드파티 쿠키 퇴출[23)]

▶ 애플에 이어 구글 또한 자사가 운영 중인 웹브라우저 크롬(Chrome)에서 서드파티 쿠키 지원을 중단하면서 서드파티 쿠키가 사실상 퇴출 수순을 밟을 것으로 전망

- 구글은 '24년 1월 초부터 크롬 브라우저 이용자의 1%를 대상으로 서드파티 쿠키를 차단 테스트에 돌입

- 이는 '24년 서드파티 쿠키의 완전한 지원 중단에 앞선 단계적 조치로서 약 3,000명의 이용자가 테스트 대상이 될 것으로 추산

- 이후 '24년 3분기에는 모든 이용자를 대상으로 서드파티 쿠키 차단이 이루어질 예정

▶ 다만, 구체적인 일정은 영국 경쟁시장청(Competition and Markets Authority)이 구글에 제기한 독점금지 관련 문제를 구글이 언제 해소할 수 있느냐에 따라 변동의 여지가 있음

- 영국 경쟁시장청은 구글의 쿠키 지원 중단이 디지털 광고 부문에서의 경쟁을 심각하게 저해할 수 있다고 우려를 표명

- 이는 디지털 광고 사업자가 이용자의 개인화된 온라인 활동 정보를 수집하지 못하므로, 광고 사업자 입장에서는 이용자에게 맞춤형 광고를 제공하기 위해 구글 이용자 데이터베이스에 더욱 의존할 수밖에 없는 상황에 직면하기 때문

23) The Register, Google's third-party cookie culling to begin in Q1 2024 ... for 1% of Chrome users, 2023.10.12.

Reference

1. 개인정보보호위원회. 개인정보 보호 기본계획(2024-2026), 2023.6.28.
2. 개인정보보호위원회, 신뢰 기반 인공지능 데이터 규범, 첫 발 떼다, 2023.8.3.
3. 개인정보보호위원회, 전면 개정 개인정보 보호법, 9월 15일 시행, 2023.9.5.
4. 금융위원회, [보도자료] 지속가능한 마이데이터 기반 마련을 위해 합리적 과금체계 구축, 2023.12.7.
5. 뉴시스, 굿닥·닥터나우 등 비대면 진료 앱 5개社 과태료 처분..."개인정보 관리 허술", 2023.5.10.
6. 뉴시스, 내달부터 '청소년 잊힐권리' 시행..."내 SNS 퍼간 제3자 게시글도 삭제 가능", 2023.3.6.
7. 메디칼타임즈, 수술실 CCTV 가이드라인 나왔다...혼란 잦아들까, 2023.9.6.
8. 보안뉴스, 개인정보위, '개인정보 국외 이전 운영 등에 관한 규정' 10월 16일 제정·시행, 2023.10.12.
9. 보안뉴스, CCTV 영상정보 활용: 실무적 접근을 위한 개인정보보호법 해석_①개요, 2023.9.6.
10. 서울신문, [법안 톺아보기] CCTV에 찍힌 사생활 지켜줄 '개인영상정보 보호법', 이번에는 통과될까? 2023.9.22.
11. 아시아경제, 개인정보 자기결정권 실현 '마이데이터', 첫 걸음, 2023.8.17.
12. 의약뉴스, "의료 마이데이터 구현 위해 개인건강정보 이동권 보장해야", 2023.9.26.
13. 전자신문, 개인정보위, AI 시대 개인정보 보호 정책 발표...전담팀 신설, 2023.8.3.
14. 지디넷코리아, 오픈AI, 국내 첫 개인정보 보호 위반 제재, 2023.7.27.
15. 테크월드뉴스, 온라인 플랫폼 규제 '양날의 검'… 데이터 주권 이상 없나, 2023.12.29.
16. 한겨레, '틱톡 사태'로 고민 깊은 정부...'개인정보 국외이전' 통상 압력 어쩌나, 2023.4.20.
17. BigID, 10 Data Privacy Predictions for 2024 & Beyond, 2023.12.7.
18. Davis+Gilbert LLP, California's Age-Appropriate Design Code Blocked on Constitutional Grounds, 2023.10.2.
19. Deloitte, Data Protection: E-book Privacy Enhancing Technologies(PETs) EU and UK overview, 2023.10.
20. eucrim, CJEU: Systematic Collection of Biometric and Genetic Data Contrary to EU Law, 2023.2.15.
21. Harvard Business Review, 3 Obstacles to Regulating Generative AI, 2023.10.31.
22. iapp, US State Privacy Legislation Tracker, 2023.12.22.
23. JD Supra, 5 Emerging Data Privacy Trends in 2024, 2023.12.14.
24. OECD, Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches. 2023.3.
25. Reuters, Japan privacy watchdog warns ChatGPT-maker OpenAI on user data, 2023.6.2.
26. TechCrunch, Poland opens privacy probe of ChatGPT following GDPR complaint, 2023.9.21.
27. The Register, Google's third-party cookie culling to begin in Q1 2024 ... for 1% of Chrome users, 2023.10.12.
28. The Verge, Italian regulators order ChatGPT ban over alleged violation of data privacy laws, 2023.3.31.
29. The Verge, 'Modern cars are a privacy nightmare,' the worst Mozilla's seen, 2023.9.6.
30. The White House, FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, 2023.10.30.
31. 読売新聞, 生成ＡＩ開発、第三者が認証する仕組み創設検討...リスク軽減へ規制強化, 2023.11.7.

<2023년 개인정보보호 월간 동향 보고서 발간 목록>

번호	호수	제 목
1	1월 01	주요국 개인정보보호 강화기술 정책동향 분석 및 시사점
2	1월 02	EU 인공지능법(안)과 GDPR의 상호작용 분석
3	1월 03	해외 아동 개인정보 보호 침해 관련 행정처분 사례 분석
4	2월 01	해외 경쟁법 관련 개인정보보호 이슈 분석
5	2월 02	미국의 개인정보보호 법제 입법 동향
6	2월 03	디지털 자산과 개인정보보호의 관련성 및 고려사항
7	3월 01	웹 3.0 시대 도래로 부상하는 개인정보보호 이슈 분석
8	3월 02	사우디아라비아의 데이터·프라이버시 규제 샌드박스 추진현황
9	3월 03	개인정보보호와 활용성 강화 기술로 주목받는 재현데이터 기술의 특성과 활용 과제
10	4월 01	2023년 주요 개인정보보호 실태 서베이 보고서 분석
11	4월 02	ChatGPT의 등장과 주요국의 개인정보보호 규제 동향
12	4월 03	2022년 4분기 EDPB 총회 주요 결과 분석
13	5월 01	해외 주요 개인정보 감독기관 연례보고서 주요 내용 및 활동성과
14	5월 02	EDPS 2022 연간 활동 보고서 분석
15	5월 03	안면인식기술 제재 관련 정책 추진 및 분석과 평가
16	6월 01	2023년 상반기 개인정보 규제 위반에 대한 해외 주요국 제재 및 처분 사례 분석
17	6월 02	EDPB의 개인정보 역외 이전 지침 주요 내용 분석
18	6월 03	영국 개인정보 감독기관(ICO)의 DSAR 기업 대응 지침 분석 및 평가
19	7월 01	미국의 소비자 건강·의료 개인정보 침해 사례와 입법 동향 분석
20	7월 02	국내외 정보주체 삭제권(잊힐 권리) 강화 동향
21	7월 03	CCTV 설치·운영에 관한 최근 개인정보보호 주요 지침과 이슈 분석
22	8월 01	EU집행위원회의 '웹 4.0 및 가상세계 전략'으로 본 EU의 메타버스 개인정보 보호 이슈 및 대응 동향
23	8월 02	Apple · Goolge의 서드파티 쿠키 퇴출 정책 현황 분석
24	8월 03	EU-미국 데이터 프라이버시 프레임워크[DPF] 주요 내용 및 시사점

25	9월 01	미국 데이터브로커 관련 규제 및 정책 동향
26	9월 02	데이터 스크래핑에 대한 12개 개인정보 감독기관의 공동 성명 발표와 관련 주요 이슈
27	9월 03	유럽 DSA와 개인정보보호 규제당국의 주요 역할 분석
28	10월 01	TiKTok의 아동 개인정보 위반에 대한 DPC 제재 및 최종 결정 분석
29	10월 02	GDPR 체계 하에서의 AI 챗봇 관련 개인정보 이슈 분석
30	10월 03	아동·청소년 개인정보보호 관련 정책 동향
31	11월 01	해외 주요국 개인정보 감독기관 연례보고서 주요 내용 및 활동 성과(2)
32	11월 02	뉴로 기술 발전으로 인해 새롭게 부상하는 개인정보보호 이슈 분석
33	11월 03	2023년 주요 개인정보보호 실태 서베이 보고서 분석
34	12월 01	개인정보보호 분야 국제조직(IAPP,GPA,FPF) 주요 활동 및 논의 내용 분석
35	12월 02	2023년 하반기 주요 개인정보보호 위반에 대한 해외 주요국 제재 및 처분 동향
36	12월 03	2023년 국내외 개인정보 이슈 점검과 2024년 주요 이슈 전망

2023

개인정보보호 월간동향분석 제12호

발 행 2023년 12월 29일

발행처 한국인터넷진흥원
개인정보본부 개인정보정책팀
전라남도 나주시 진흥길 9
Tel: 061-820-1865

1. 본 보고서는 개인정보보호위원회 「개인정보보호 동향 분석」 사업 수행 결과물입니다.

3. 본 보고서의 내용은 한국인터넷진흥원의 공식 입장과는 다를 수 있습니다.