2023 Privacy Report

개인정보보호 월간동향분석

8월호

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2023 Privacy Report

개인정보보호 월간동향분석

8월호

1. EU집행위원회의 '웹 4.0 및 가상세계 전략' 으로 본 EU의 메타버스 개인정보 보호 이슈 및 대응 동향 분석

2. Apple · Google의 서드파티 쿠키 퇴출 정책 현황 분석

3. EU-미국 데이터 프라이버시 프레임워크[DPF] 주요 내용 및 시사점

KISA

EU집행위원회의 '웹 4.0 및 가상세계 전략'으로 본 EU의 메타버스 개인정보 보호 이슈 및 대응 동향 분석

[목 차]

1. 개요

▶ EU집행위원회(EC)는 EU의 차세대 기술 전환을 주도하고 EU 시민, 기업 및 공공 행정기관의 디지털 환경 개방성·안전성·신뢰성·공정성·포용성을 보장하기 위한 '웹 4.0* 및 가상세계** 전략[1] 문서'를 공개('23.7)

* 개방성, 탈중앙화, 사용자의 완전한 권한 부여 등을 주요 특징으로 최근 진전을 보이고 있는 웹 3.0을 넘어 다음 세대인 웹 4.0은 디지털과 실제 사물 및 환경 간의 통합, 인간과 기계 간의 향상된 상호 작용을 가능하게 하는 웹 개념

** 다양한 목적으로 물리적 세계와 디지털 세계를 실시간으로 혼합할 수 있는 3D 및 확장현실(XR) 등의 기술을 기반으로 하는 지속적이고 몰입감 있는 환경

1) European Commission, Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds, 2023.7.11.

- EU의 경제전망 자료에 따르면, 전 세계 가상세계 시장 규모는 '22년 270억 유로에서 '30년 8,000억 유로 이상으로 성장할 것으로 전망

- 이 문서에서 EU 정부는 디지털화를 향후 EU 경제 성장의 주요 동력 중 하나로 인식하고 있으며, 웹 4.0은 원활하게 상호 연결된 지능형 몰입형 세상을 구현하기 위한 중요한 전환 기술임을 강조

▶ 이번 전략 문서는 메타버스 기술의 발전 시 중요하게 고려되어야 할 사항으로서 아동의 권리 보호에 관한 문제와 가상세계 및 웹 4.0 개발을 위한 제도적 토대로서의 입법 체계에 대해서도 비중 있게 다루고 있음

- EU는 '아동을 위한 더 나은 인터넷 신전략(Better Internet for Kids, BIK+)', 'EU 아동 권리 전략(EU Strategy on the Rights of the Child)' 등을 언급하며, 현 시점 메타버스 시장의 주요 소비층인 아동의 인권과 개인정보 보호를 위한 조치를 강조

- 또한, 메타버스 발전을 위한 기반 제도로서 ▲GDPR ▲데이터법(Data Act) ▲암호자산 시장법(MiCA, Markets in Crypto-Assets) ▲유럽 디지털 신원(The European Digital Identity) 이니셔티브 등 다양한 입법 및 정책적 시도에 관해서도 기술

▶ 또한 이 문서는 가상세계의 발전이 아동의 권익, 개인정보 및 프라이버시 보호, 허위정보, 사이버보안, 사이버 범죄, 사이버 폭력, 차별, 배제, 혐오 발언, 소비자 보호 및 안전 등 민주 사회의 기본권과 공익에 저해되는 문제 발생 가능성이 높다고 지적

- 이외 메타버스 이해관계자 간의 책임과 의무 및 계약에 관한 규칙 수립이나, 고용 분야에서는 가상세계 사용자에게 더 낮은 기준을 부과하는 등 EU의 사회적 기준을 회피하려는 시도가 발생할 위험도 함께 언급

▶ 이하 본 고에서는 웹 4.0 및 가상세계 전략 문서 내 4대 핵심요소에 대한 주요 내용을 소개하고, 아동 권리 이슈와 다양한 메타버스 관련 법률 프레임워크에 대해 개인정보 보호 관점에서 EU 정부가 추진 중인 작업과 방향성을 개괄, 분석하고자 함

2. 전략 문서 4대 핵심 요소

▶ '웹 4.0 및 가상세계 전략 문서'는 (1) 사람 및 기술, (2) 비즈니스, (3) 정부(공공 서비스 및 프로젝트), (4) 거버넌스의 4대 핵심 요소(pillars)와 하위 실천 사항으로 구성

- 이중 (1)~(3)은 EU의 '디지털 10년(Digital Decade)'에서 제시된 '30년 디지털 목표의 주요 항목과 동일하게 구성되며, (4)는 컴퓨팅, 클라우드, 에지 등을 포함한 접속 패키지(Connectivity Package) 프로그램('23.2)*의 연장선에서 제시[2)]

* 유럽의 인터넷 접속 환경을 혁신하여 광섬유 통신 및 5G 등 고용량 네트워크 제공을 촉진하기 위한 이니셔티브

- 전략 문서는 현재 상황, 기회와 도전 과제, 목표 달성에 필요한 정책 조치에 대해 종합적으로 분석하고 있으며, 전략의 실행, 모니터링 및 평가를 위한 로드맵도 제시

(1) 사람 및 기술(skills)

▶ EU집행위원회는 EU 내 웹 4.0 및 가상세계 분야의 전문가를 육성하고 일반 대중의 이러한 기술에 대한 지식과 인식 제고를 도모

- 자금 지원 프로그램인 디지털 유럽 프로그램(Digital Europe Programme) 및 크리에이티브 유럽(Creative Europe)을 통해 개발자와 콘텐츠 크리에이터로 구성된 유럽 인재 풀을 구축하며, EU 외부로부터의 숙련된 전문가 유치 역시 정책 우선순위

- 집행위원회는 가상세계 '툴박스(Toolbox)' 개발을 통해 가상 신원, 창작물, 디지털 지갑 솔루션 등의 자산 및 데이터를 관리 방안, 개인정보 보호, 소비자 보호, 사이버 보안, 저작권 및 지적 재산, 허위 정보 방지 방안을 포함하여 가상세계에 대한 대중의 이해를 증진할 계획

  - 툴박스는 유럽 디지털 미디어 관측소(European Digital Media Observatory)* 및 허위 정보에 관한 실천 강령(Code of Practice on Disinformation)** 등의 기존 프로그램의 일환으로 추진

* 허위 정보에 대응 활동을 펼치는 독립 커뮤니티를 지원하기 위한 프로젝트로, 팩트 체커(checker)를 비롯해 학계 및 기타 관련 이해관계자들이 서로 협력할 수 있는 허브 역할을 제공

** 온라인 허위 정보 문제와 이에 따른 사회적 악영향을 해결하기 위한 EU집행위원회의 자율 규제 이니셔티브. 2018년에 구글, 페이스북, 트위터, 마이크로소프트 등 주요 온라인 플랫폼과 광고주, 팩트체커, 시민사회 단체 등 기타 이해관계자들이 최초로 채택

- 또한, 집행위원회는 조만간 연령별 디자인 코드(design code)를 통해 가상세계를 어린이 친화적으로 설계하고 '아동을 위한 더 나은 인터넷(Better Internet for Kids, BIK)' 포털을 통해 어린이들에게 보다 친숙한 가상세계 환경을 제공할 계획

  - BIK 포털은 온라인 공격, 사이버 왕따, 성적 학대, 혐오 발언 등 온라인 안전 및 디지털 시민의식과 관련된 다양한 주제에 대한 정보, 지침 및 리소스를 제공하며, EU 각국에서는 이와 관련된 인식 제고, 헬프라인, 핫라인, 청소년 참여 서비스를 제공하는 유럽의 안전한 인터넷 센터(SIC, Safer Internet Centres) 네트워크를 지원

2) EURACTIV, EU Commission launches Connectivity Package with 'fair share' consultation, 2023.2.23.

(2) 비즈니스

▶ 전략 문서는 웹 4.0과 가상세계 분야와 관련해 유럽이 기술 전문 지식의 파편화, 느린 신기술 수용, 금융 서비스에 대한 제한된 접근 등으로 인해 산업 잠재력이 저해되고 있다고 평가하며 이를 해결하기 위해 가상세계 생산 체인의 모든 단계에 걸친 주체들 간 협업을 강조

- **(새로운 유럽 파트너십, New European Partnership)** 주요 가상세계 이해관계자들 간에 첨단 기술, 유럽 데이터 공간 및 차세대 인터넷 이니셔티브에 관한 대화와 투자 협력 기회를 제공
- **(규제 샌드박스)** 개발자에게 가상세계 기술 및 서비스를 자유롭게 테스트할 수 있도록 위험 부담 없는 환경에서 규제 준수 여부를 평가할 수 있는 규제 샌드박스를 제공하고, 혁신 수용적인 비즈니스 환경을 조성
- **(공정경쟁 환경)** 대형 시장 플레이어의 가상세계 독점을 견제하고, 회원국 및 이해관계자와 함께 상호운용성 표준을 개발하여 플랫폼과 네트워크의 상호운용성을 보장함으로써 가상세계의 비즈니스 환경이 경쟁력을 유지할 수 있도록 도모

(3) 정부(공공 서비스 및 프로젝트)

▶ EU집행위원회는 중앙 및 지방 정부가 디지털화를 통해 공공 서비스의 설계 및 제공을 개선하고 건강 및 기후 변화와 같은 주요 사회적 과제를 해결하는 방향으로 웹 4.0을 추진

- **(유럽 시티버스, European CitiVerse)** 지자체의 도시 계획과 관리를 유연화하기 위한 자금 지원 프로그램으로, 민주주의, 인권, 법치, 개인정보 보호, 소비자 보호 등 EU의 가치와 원칙을 반영하는 웹 4.0 및 가상세계 기술의 개발과 채택을 촉진
- **(혁신 친화적 규제 자문 그룹, The Innovation Friendly Regulations Advisory Group)** 미래의 가상세계 공공 서비스 이니셔티브를 발굴 운영하기 위해 EU집행위원회가 '22년에 설립한 상위 정책 자문 기구로, 규제 샌드박스, 리빙랩, 테스트베드 등을 통해 AI, 블록체인, 클라우드 컴퓨팅, 5G 등 첨단 디지털 기술의 공공 서비스 활용 촉진을 도모

(4) 거버넌스

▶ EU집행위원회는 웹 4.0과 가상세계가 가져올 사회적 변화를 관리하기 위해 회원국 대표로 구성된 전문가 그룹을 소집하여 회원국 간 및 국제 포럼을 통해 모범 사례를 공유할 계획

- 기존 인터넷 거버넌스 기관의 권한을 넘어서는 가상세계와 웹 4.0의 실제적인 문제를 다루기 위해 기술 분야의 다양한 이해관계자 간 거버넌스 프로세스의 구축을 지원

- 유럽 알고리즘 투명성 센터(European Centre for Algorithmic Transparency), EU 블록체인 관측소 및 포럼(EU Blockchain Observatory and Forum) 등 기존 기구를 통해 가상세계와 웹 4.0의 새로운 발전을 모니터링하여 새로운 성장과 혁신 기회를 파악하고, 모범 사례를 장려하며, 새로운 과제식별을 도모

3. 전략 문서 내 개인정보 보호 이슈

(1) 아동 권익 및 개인정보 보호

▶ 메타버스 이해관계자들은 메타버스 플랫폼 환경 내에서의 어린이와 청소년의 안전, 보안 및 개인정보 보호, 기타 아동의 권익 보호를 위한 의무에 대한 이해 필요

- 아동은 온라인 아동 성적 학대로부터의 보호 등 아동의 복지에 필요한 보호를 받을 기본적 권리가 존중되어야 함

▶ **(아동의 권리에 관한 EU 전략[3])** 현실세계와 마찬가지로 가상세계에서도 모든 아동의 권리는 아동의 안전 조치와 프라이버시 내재화(privacy by design) 등을 통해 보장되어야 함

- 이 전략은 GDPR 등 EU의 개인정보 보호 관련 규정이 가상세계와 웹 4.0에 완전히 적용되도록 하고, 아동이 자신의 데이터를 통제하고 열람, 수정, 삭제, 이동성 등의 권리 행사를 보장하는데 목표를 두고 있음

- 아동은 생체, 행동, 감정 데이터 등 다양한 유형의 정보를 생성, 공유, 저장할 수 있는 가상세계에서 개인정보를 보호하고 잊힐 권리를 보장받을 수 있어야 함

- 프라이버시 내재화를 통해 다양한 가상세계와 플랫폼에서 차별, 조작 또는 원치 않는 광고로 이어질 수 있는 아동에 대한 추적 및 프로파일링 방지가 가능

▶ **(아동을 위한 더 나은 인터넷 신전략, BIK+[4])*** 온라인 및 가상 환경에서 아동을 보호하고 권한을 부여하기 위한 EU의 조치를 기술

* BIK의 후속 전략으로 아동의 안전한 디지털 환경 제공, 디지털 기술 역량 강화 및 아동의 권익 존중 등을 주요 목표로 '22.5월 공개된 이니셔티브

3) EC, COM(2021) 142 final: EU Strategy on the Rights of the Child, 2021.3.24
4) https://www.betterinternetforkids.eu/policy/newbikstrategy

- 보다 아동 친화적인 가상세계 구축을 위해 BIK 포털은 청소년, 학부모, 교육자를 위한 가상 환경에 대한 교육 리소스를 제공하고 EU 전역의 인터넷 안전 센터에서 인식 제고 활동을 하는 데 사용될 예정

▶ **(아동의 성적 학대 및 성적 착취 근절에 관한 지침 재개정안[5])** 가상세계와 가상세계를 통해 아동에게 가해지는 성범죄의 예방, 조사 및 처벌에 관한 내용을 다루고 있음

(2) 입법 프레임워크

▶ **(GDPR)** 메타버스 내에서의 개인정보 처리에도 일관성 있게 적용되어야 하므로, 메타버스 플랫폼은 개인정보 처리 시 정보주체의 원칙과 권리를 보호해야 할 의무가 있음

- 개인정보 처리 컨트롤러 또는 프로세서의 설립 위치 또는 정보주체의 위치에 관계없이 메타버스 내 개인정보 처리 시 GDPR을 준수(제3조)

  - GDPR은 EU 내 개인정보 주체에게 상품 또는 서비스를 제공하거나 EU 내에서 개인정보 주체의 행동을 모니터링하는 것과 관련된 모든 개인정보 처리에 적용되므로, EU 사용자를 타기팅하거나 추적하는 모든 메타버스 제공자 또는 운영자는 GDPR과 그 원칙을 준수해야 함

- 메타버스 서비스 제공자, 운영자, 개발자, 크리에이터, 사용자, 제3자 등 메타버스와 관련된 다양한 행위자의 역할과 책임을 명확히 해야 함(제24조, 제28조)

  - GDPR은 메타버스에서의 기능과 활동에 따라 서로 다른 행위자가 컨트롤러나 프로세서, 또는 둘 다의 역할을 수행할 수 있으므로, 이들은 GDPR에 따른 각자의 의무와 권리를 명확히 정의하고 이를 반영하여 계약을 체결

- 메타버스 서비스 제공사는 정보주체의 개인정보에 대한 열람권(제15조)·정정권(제16조)·삭제권(제17조)·제한권(제18조)·이동권(제20조)·반대할 권리(제21조)·차별 금지권(제22조) 등 다양한 권리를 부여해야 함

  - 즉, 메타버스 사용자는 메타버스 공간 내에서 자신의 개인정보가 어떻게 수집되고 사용되는지에 대한 정보를 제공받아야 하며 언제든지 자신의 정보를 열람, 수정, 삭제 또는 전송할 수 있어야 함

- 메타버스 서비스 제공사는 특수 범주의 개인정보(민간 정보) 처리를 위한 구체적인 안전 조치를 적용해야 함(제9조)

5) EC, Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children, and child pornography,

- GDPR은 특수 범주의 개인정보를 인종 또는 민족, 정치적 견해, 종교 또는 철학적 신념, 노동조합 가입 여부, 유전자 데이터, 개인을 고유하게 식별하는 생체 데이터, 건강 데이터, 개인의 성생활 또는 성적 취향에 관한 데이터를 드러내는 데이터로 정의

- 메타버스 서비스 제공사는 이러한 정보를 처리하기 전에 사용자로부터 유효한 동의를 얻어야 하며, 무단 액세스 또는 공개로부터 개인정보를 보호하기 위한 추가 보안 조치를 강구해야 함

• 메타버스의 설계 및 기본 설정을 통해 개인정보 보호 수준을 증진시켜야 함(제25조)

- GDPR은 컨트롤러에게 개인정보 처리의 전체 수명 주기 동안 높은 수준의 개인정보 보호를 보장하기 위해 적절한 기술적 및 조직적 조치를 마련하도록 요구

- 즉, 메타버스 행위자는 제품 및 서비스를 설계하고 개발하는 초기 단계부터 개인정보 보호에 미치는 영향을 고려하고 개인정보 보호 강화 기능을 포함해야 함

- 또한 기본적으로 각 목적에 필요한 최소한의 개인정보만 처리하도록 해야 함

▶ **(EU 데이터법안[6])** 다양한 부문과 영역에서 정보 열람 및 사용에 대한 조화로운 규칙을 수립하여 EU에서 공정하고 경쟁력 있는 데이터 경제를 조성하는 것을 목표로 한 법률안으로, 메타버스 관점에서 동 법안의 해석을 적용한 내용은 다음과 같음

• '설계에 의한 개인정보 보호' 개념 하에 메타버스 제공자와 운영자가 데이터 처리의 전체 수명 주기 동안 높은 수준의 개인정보 보호를 보장(전문(7))

• 메타버스 상에서의 개인정보 처리는 적법성, 공정성, 투명성, 목적 제한, 데이터 최소화, 정확성, 저장 제한, 무결성, 기밀성, 책임성 등의 GDPR 및 그 원칙을 준수해야 함(제5조)

• 정보주체는 GDPR 제17조에 따라 자신의 개인정보 삭제를 요청할 권리가 있음(제6조)

• 메타버스 제공자와 운영자는 복수의 여타 플랫폼에서의 추적 및 프로파일링의 가능성과 결과에 대해 사용자에게 알리고, 그러한 관행에 참여하기 전에 사용자의 명시적인 동의를 얻도록 요구(제5조)

• 메타버스 상에서의 전자통신 데이터 처리는 기밀성, 보안, 동의, 투명성과 같은 전자 개인정보 보호 규정(ePrivacy Directive)과 그 원칙을 준수(전문(32))

▶ **(암호자산시장법, MiCA[7])** 기존 EU 금융 서비스 법률 프레임워크에서 명확히 다뤄지지 않는 암호화 자산(토큰) 및 거래를 규제하기 위한 법안으로, 메타버스 내에서 발생될 수 있는 거래와 관련된 규정은 다음과 같음

6) Data Act, Proposal for a Regulation COM/2022/68 final, 2022.2.23. EU 데이터법안은 2023년 6월 27일 유럽의회, 이사회, 집행위원회가 삼자 합의를 이루었으며 연내 제정될 예정
7) Regulation (EU) 2023/1114, Markets in Crypto-Assets (MiCA) Regulation

- 암호화 자산 거래 플랫폼(Crypto-Asset Trading Platform) 상에서 암호화 자산 거래 시 공정하고 질서 있는 거래를 보장하고 시장 남용을 방지하도록 규정(제14조)
- 암호화 자산 서비스 제공자(CASP, Crypto-Asset Service Providers)와 암호화 자산 발행자(CAI, Crypto-Asset Issuers)의 활동 및 의무와 관련한 인가 및 감독(제16조, 제18조)
- 자산 및 자산 소유자의 보호, 무결성, 투명성과 관련하여 CASP와 CAI의 법적 지위와 책임을 정의(제17조)
- 자본 요건, 거버넌스 체계, 리스크 관리 절차, 내부 통제 등 CASP와 CAI에 대한 건전성 요건을 규정(제34조)

▶ **(유럽 디지털 신원, The European Digital Identity)** EU 시민, 거주자 및 기업이 사용할 수 있는 안전하고 신뢰할 수 있는 디지털 신원 프레임워크를 구축하기 위한 이니셔티브로, 사용자에게 자신의 정보에 대한 통제 하에 온/오프라인의 다양한 서비스와 공유하기 위해 다음의 방안들을 제시

- 개인 디지털 지갑(wallet)을 통해 사용자는 국가 신분증, 여권, 운전면허증과 같은 전자 식별 수단과 졸업장, 은행 계좌, 의료 기록과 같은 기타 개인정보를 저장하고 관리
  - 디지털 지갑은 공통 기술 표준을 기반으로 하며 EU 전역에서 상호운용성을 확보
- 사용자 중심 접근 방식을 개발 및 채택하여 사용자가 다양한 서비스와 얼마나 많은 정보를 공유할지 결정하고 언제든지 동의를 제공하거나 철회할 수 있는 메커니즘을 제공
  - 또한 디지털 지갑은 사용자에게 개인정보가 어떻게 그리고 누구에 의해 사용되는지에 대한 투명성과 피드백을 제공할 수 있을 것
- 암호화, 허가, 검증, 인증 및 감사 등의 적절한 기술 및 조직 차원의 조치를 구현하여 사이버 공격 및 사기에 대한 디지털 신원 시스템의 보안 및 복원력을 강화
  - 디지털 지갑은 사용자에게 개인정보 유출 발생 시 통보 기능을 제공

4. 전망과 평가

▶ EU집행위원회의 웹 4.0 및 가상세계 전략 문서는 향후 유럽의회 및 EU이사회의 승인을 거쳐 확정될 예정으로 향후 12개월 동안 세부 실행 과제에 대한 보완 논의가 지속될 것으로 예상

▶ 이 문서는 메타버스의 본격적 확산을 앞두고 민간, 공공, 시민 등 다양한 영역에서 발생될 수 있는 이슈와 대비 사항을 개괄적으로 점검하며 필요한 정책 수단 개발과 사회적 합의를 위한 실무적인 조언을 제공

- 전략 문서는 단일 법률 단위에서 포괄적으로 규정되지 않는 메타버스(=웹 4.0 및 가상세계) 분야의 개인정보 보호 관련 규제에 대해 이미 입법이 완료되거나 추진 중인 다양한 법률 프레임워크를 개괄적으로 제시함으로써 구체적 후속 논의를 이어 나가기 위한 방향을 제시

▶ 지역적 범위를 넘어서는 메타버스가 개인정보를 포함한 시민의 가치를 옹호하고 기존 규칙을 존중하는 개방적이고 안전한 공간으로 형성되기 위해서는 향후 보다 폭넓은 국제적 논의가 필요

- 이를 통해 메타버스 내 개인정보 보호의 기초를 형성하는 상호운용성, 신원 관리 또는 네트워크 표준 등의 기술적 문제에서부터 개인정보 처리 전반에 걸친 광범위한 주제에 대한 국제적 공감대 형성과 세부 이슈 발굴이 필요

Reference

1. EC, Data Act- Proposal for a Regulation COM/2022/68 final, 2022.2.23
2. EC, COM(2021) 142 final: EU Strategy on the Rights of the Child, 2021.3.24
3. EC, Towards the next technological transition: Commission presents EU strategy to lead on Web 4.0 and virtual worlds, 2023.7.11.
4. EU, Regulation (EU) 2016/679, General Data Protection Regulation, 2016.4.27
5. EU, Regulation (EU) 2023/1114, Markets in Crypto-Assets (MiCA) Regulation, 2023.6.9

Apple · Google의 서드파티 쿠키 퇴출 정책 현황 분석

[목 차]

1. 개요

▶ 쿠키(cookie)는 인터넷 브라우저 방문자가 웹사이트 접속 시 컴퓨터나 모바일 장치에 내려받게 되는 작은 텍스트 파일로, 방문자의 온라인 행태정보 등을 저장

- 쿠키는 발행 주체에 따라 크게 퍼스트파티 쿠키(First-Party Cookie)와 서드파티 쿠키(Third-Party Cookie)로 구분
- 대부분의 경우 쿠키는 별도의 보안 위험을 초래하지 않으나, 일부 쿠키에서 수집된 정보가 사용자의 명확한 동의 없이 제3자에게 제공되는 것에 대해 개인정보보호 및 온라인 사생활 보호 침해 논란이 발생

표 _ 퍼스트파티 쿠키 및 서드파티 쿠키의 구분

구분	개념
퍼스트파티 쿠키	• 웹사이트를 소유하는 주체가 직접 생성하는 쿠키 • 웹사이트 소유자는 이를 통해 웹사이트 내 언어 기본 설정, 로그인 세부 정보, 장바구니에 추가된 제품 등 웹사이트 방문자의 행태정보를 기억하는 데 사용
서드파티 쿠키	• 웹사이트 소유자가 아닌 제3자(예, 디지털 광고기술 기업, 소셜 미디어 사이트 등)에서 발행한 쿠키 • 서드파티 쿠키를 통해 제3자가 소비자의 행동, 이동 경로 등을 파악할 수 있으며, 주로 교차 사이트 추적(Cross-Site Tracking)* 및 리타기팅(retargeting)**과 같은 행동기반 타기팅에 활용 * 사용자가 한 웹사이트에서 다른 웹사이트로 이동할 때 광고 회사나 데이터 수집 업체가 여러 웹사이트에 걸쳐 사용자의 활동을 추적하여 광고를 맞춤화하는 것을 지칭 ** 웹사이트를 방문한 사용자의 과거 상호 작용을 기반으로 사용자가 관심을 보였던 제품의 광고를 표시하는 온라인 마케팅 기법

▶ 각 산업 분야에서 급격히 이루어지고 있는 디지털화에 따라 온라인 개인정보보호 이슈가 전 세계적으로 강화되는 추세이며, 이에 많은 국가와 지역에서는 쿠키 사용에 대한 규제와 개인정보보호에 관한 법률을 시행

• 일명 'EU 쿠키법'으로도 불리는 ePrivacy 지침[8]은 웹사이트 운영자가 웹사이트에서 쿠키 및 유사한 기술 사용에 대해 명확하고 포괄적인 정보를 제공해야 하며, 필수적이지 않은 쿠키와 개인정보보호에 적합하지 않은 분석 쿠키를 설정하기 전 사용자의 동의를 얻어야 한다고 규정

• ePrivacy 지침을 계승한 EU 일반 개인정보보호법(이하 GDPR)[9] 또한 개인정보 활용에 대한 사용자의 동의 없는 개인정보의 수집을 금지

- '18년 5월 GDPR의 시행은 웹사이트에서 쿠키 사용 동의 여부 등을 묻는 쿠키 팝업*(또는 쿠키 배너)의 노출을 활성화하는 계기가 됨[10]

* cookie popup: 사용자가 웹사이트를 첫 방문 시 웹사이트에 표시되는 그래픽 알림으로, 웹사이트가 쿠키 및 기타 추적 기술을 사용하여 데이터를 수집한다는 사실을 방문자에게 알리고, 사용자의 장치에 쿠키를 저장하는 데 동의를 요청

• GDPR 이외에 미국 캘리포니아주 소비자 개인정보보호법(CCPA)[11], 브라질 일반 개인정보보호법(LGPD), 프랑스 개인정보보호법(LIL),[12] 남아프리카공화국 개인정보보호법(POPIA) 등에서도 정보주체의 동의 요건을 명시

8) Directive on Privacy and Electronic Communications (Directive 2002/58/EC)
9) General Data Protection Regulation (Regulation 2016/679)
10) 이는 EU 내 웹사이트가 ePrivacy 지침 및 GDPR의 적용을 받기 때문이며, GDPR 시행 이후 쿠키 동의 요건은 법적 구속력을 갖추게 됨. 따라서 EU 국가에서 작동하는 웹사이트이거나 해당 국가 방문자가 있는 경우 규정 준수를 위해 쿠키 팝업 또는 배너를 배치해야 함
11) California Consumer Privacy Act
12) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

- 이와 같은 개인정보보호 인식 제고를 통해 쿠키 추적에 대한 대중의 저항이 커지고 있는 한편, 매번 쿠키 수집 동의를 요청하는 쿠키 팝업의 확산에 전 세계 사용자의 피로감 또한 높아진 상황

  - EU 집행위원회는 온라인 사용자에게 지속적으로 동의를 요청하는 현행 시스템으로 인해 '쿠키 피로감'이 발생하고 있다고 지적

▶ GDPR 시행 이후 개인정보보호 규정 준수에 대한 압박이 증가하자, Apple, Google, Mozilla, Microsoft 등 글로벌 웹브라우저 운영사들은 서드파티 쿠키 차단 수순을 밟고 있음

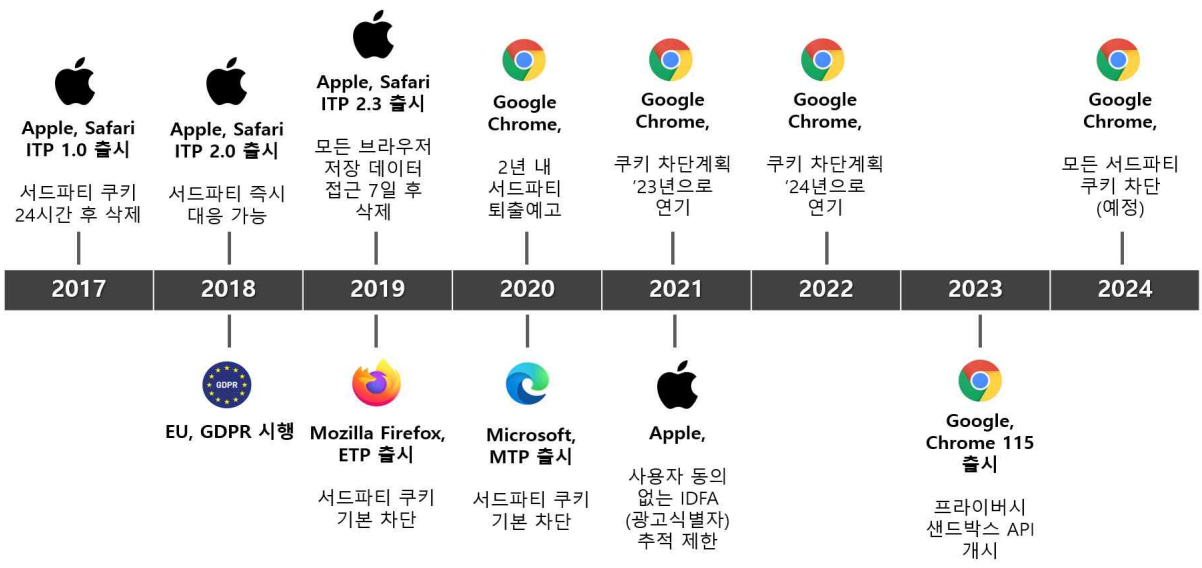
- Apple은 쿠키 차단 선두주자로서 '17년부터 자사 웹브라우저 Safari에서 서드파티 쿠키를 사실상 무력화 조치

- 웹브라우저 시장 점유율 1위를 차지한 Chrome의 운영사 Google 또한 '20년 1월, 서드파티 쿠키에 대한 지원을 2년 내로 중단하겠다고 발표

※ 그러나 Chrome의 서드파티 쿠키 퇴출 계획은 두 번에 걸쳐 연기됐으며,[13][14] '24년에야 온전히 이행될 예정

- Mozilla는 '19년 6월 사용자 설정에 따라 서드파티 쿠키를 자동 제한하는 Enhanced Tracking Prevention(ETP) 기술을 웹브라우저 Firefox에 도입했으며, Microsoft 또한 '20년 1월부터 유사한 Microsoft Tracking Prevention(MTP) 기술을 Edge에 적용

그림 _ 주요 웹브라우저별 서드파티 쿠키 퇴출 타임라인



▶ 이하 본고에서는 쿠키 차단 선두주자인 Apple Safari와 웹브라우저 시장 점유율이 가장 높은 Google Chrome의 서드파티 쿠키 퇴출 현황을 대표적으로 소개하고, 해외 개인정보 감독기관들의 서드파티 쿠키 관련 규제를 다루고자 함

13) https://www.marketing-interactive.com/analysis-googles-third-party-cookies-wipe-out-delay-to-2023-sends-industry-lifeline-say-adtech-pros
14) https://techcrunch.com/2023/05/18/google-will-disable-third-party-cookies-for-1-of-chrome-users-in-q1-2024/

2. Apple과 Google의 탈(脫) 쿠키 정책

(1) Apple Safari의 'Intelligent Tracking Prevention(ITP)' 도입 및 업데이트 현황

▶ '17년 9월, Apple은 자사 Safari 브라우저에서 사용자의 행동 추적을 제한하고 개인정보 보호를 강화하기 위해 머신러닝 기반의 Intelligent Tracking Prevention(이하 ITP) 기능을 출시

- **(ITP 1.0)** '17년 공개된 ITP 초기 버전은 교차 사이트 추적을 방지하기 위해 서드파티 쿠키의 수명을 24시간으로 제한했으며, 웹 사용자가 30일 동안 해당 도메인과 상호 작용하지 않는 경우 자동으로 해당 쿠키를 삭제
  - 그러나 사용자가 24시간 이내에 웹사이트에 접근하지 않을 경우 추적이 차단되며 동영상 구독 서비스 및 서드파티 결제 제공업체가 영향을 받자, Apple은 ITP 1.1 업데이트를 통해 Facebook 같은 퍼스트파티 서비스에 이미 로그인한 사용자를 인증할 수 있도록 조치
- **(ITP 2.0)** '18년 6월, Apple은 ITP 2.0 업데이트를 통해 기업이 사용자를 추적할 수 없도록 조치하고, Storage Access API를 통해 사용자가 쿠키를 관리할 수 있도록 제공[15)]
  - 즉, 기존 ITP 1.0과 ITP 1.1에서 허용했던 24시간 서드파티 쿠키 추적 기능사용을 차단하여, 기업들이 리타기팅 목적으로 쿠키를 사용자 브라우저에 남기는 것이 불가능해짐
  - 또한 추적형 쿠키를 발견하면 사용자에게 확인 메시지를 표시하여, 사용자가 허용한 쿠키는 서드파티 쿠키라 할지라도 차단되지 않도록 개량
- **(ITP 2.1)** Apple은 '19년 2월, JavaScript의 'Document.cookie API'를 통해 생성된 퍼스트파티 쿠키 또한 7일 이내 삭제되도록 조치하고, 대부분의 서드파티 쿠키들의 사용이 더 이상 불가능하도록 ITP를 업데이트
  - **(ITP 2.2)** ITP 2.1 발표로부터 불과 2개월 후, Apple은 퍼스트파티 쿠키의 유지기간을 7일에서 1일(24시간)로 단축
  - **(ITP 2.3)** '19년 9월, Apple은 규제 범위를 확대하여 쿠키와는 별개의 웹사이트 데이터 저장 방식인 local storage에 저장된 데이터 또한 7일 경과 후 삭제되도록 업데이트
- 이후에도 Apple은 '20년 ITP 업데이트를 통해 Safari 브라우저에서 기본적으로 ITP를 활성화하여 다수의 웹사이트 간 사용자 추적을 차단할 수 있게 조치[16)]

15) https://webkit.org/blog/8311/intelligent-tracking-prevention-2-0/
16) https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/

- 더불어 사용자가 기본 기능 이외에 추가적으로 개인정보보호 수준을 강화하고자 할 때에는 ▲교차 사이트 추적 방지(Prevent Cross-Site Tracking) 옵션 ▲모든 쿠키 차단(Block all cookies) 옵션을 선택할 수 있도록 제공

- ITP 기술을 접목해 사용자가 자주 찾지 않는 웹사이트 쿠키를 자동으로 삭제 및 차단함으로써 동 업데이트는 Safari에서 서드파티 쿠키를 사실상 퇴출

▶ 한편 Apple은 '21년 출시한 iOS 14.5 버전부터 '앱 추적 투명성(AppTracking transparency, ATT)' 프레임워크를 장착하여 IDFA* 추적에 대한 알림을 필수적으로 띄우도록 업데이트[17]

* Identifier for Advertisers: Apple이 iOS 사용자 기기에 할당한 임의의 기기 식별자로, 광고주가 광고에 대한 사용자의 클릭, 다운로드 및 구매 여부 등 상호작용을 추적할 수 있게 해준다는 점에서 서드파티 쿠키와 유사한 기능을 수행

• 이로써 IDFA를 사용하기 위해서는 사용자 동의를 필수적으로 얻어야 하며, 사용자가 이와 같은 추적에 동의하지 않은 경우 IDFA의 사용이 불가능함

(2) Google 프라이버시 샌드박스 도입 현황

▶ Google은 '19년 8월, 서드파티 쿠키에 대한 대체재로 '프라이버시 샌드박스(Privacy Sandbox)'*의 출시 계획을 발표

* Privacy Sandbox: 서드파티 쿠키 또는 기타 추적 메커니즘 없이 교차 사이트 사용 사례를 충족시켜주는, Google의 개인정보보호 강화 기능

• **(타임라인)** '23년 7월 중순, Google은 'Chrome 115'를 정식 출시함으로써 프라이버시 샌드박스를 본격적으로 개시

- 동 계획은 본래 '23년 1월부터 적용될 예정이었으나, Google은 디지털 광고 업계에 일으킬 큰 파장을 감안하여 이와 같이 연기 결정

- Google은 ▲'23년 4분기에 레이블 옵트인(Opt-in) 테스트를 진행하고 ▲'24년 초 Chrome 사용자의 1%를 대상으로 서드파티 쿠키를 차단하며 ▲'24년 3분기까지 모든 사용자를 대상으로 완전히 서드파티 쿠키를 차단함으로써 서드파티 쿠키를 단계적으로 폐지할 계획[18]

- 따라서 이번에 활성화된 프라이버시 샌드박스는 당분간 브라우저에서 서드파티 쿠키와 공존할 예정이며, 애드테크(Ad Tech)* 업계는 '23년 7월부터 시작해 9월 20일 종료 예정인 동 시범 운영을 통해 서드파티 사용 중단에 대한 준비 여부 평가가 가능

* 광고와 기술의 합성어로, 디지털·모바일·빅데이터 등 IT 기술을 접목한 광고 기법을 의미

17) https://support.apple.com/en-us/HT212025#:~:text=App%20Tracking%20Transparency%20allows%20you,or%20sharing%20with%20data%20brokers.
18) https://techcrunch.com/2023/07/20/google-starts-the-ga-rollout-of-its-privacy-sandbox-apis-to-all-chrome-users/

- **(목적)** Google의 프라이버시 샌드박스 개발 목적은 ▲사용자의 개인정보를 보호하고 은밀한 추적을 방지하는 동시에, ▲광고로 수익을 창출하는 웹을 지원하기 위해 새로운 디지털 광고 도구를 개발함으로써 웹에서 개인정보보호를 근본적으로 강화하기 위한 일련의 공개 표준을 개발하고자 하는 데에 있음

- **(작동 원리)** 프라이버시 샌드박스는 웹퍼블리셔가 접근할 수 있는 일련의 Google 인터페이스(일명 API)로 구성

  - 이를 통해 웹 퍼블리셔들은 서드파티 쿠키 종료로 인해 발생할 수 있는 기술적 제약을 피하면서 맞춤형 광고를 계속 제공하는 것이 가능

  - 예를 들어, Google은 API 제공을 통해 ▲(FLoC API) '유사한 특성을 가진 집단'(cohorts)을 기준으로 한 사용자 분류 ▲(Topics API) 사용자 기록 분석을 통한 관심 분야 추론 ▲(Attribution reporting API) 구매 행위와 사용자가 본 광고와의 연결 등을 가능하게 함

▶ '23년 7월 12일, 프랑스 개인정보 감독기관(CNIL)은 Google의 프라이버시 샌드박스에 대한 지침을 발표하여, 프라이버시 샌드박스와 관련한 주요 안내 사항 및 권장 사항을 Chrome 사용자들에게 제시

- **(프라이버시 샌드박스 실험 참여 여부 확인)** 프라이버시 샌드박스 실험 단계에 포함된 Chrome 사용자는 무작위로 선정되며, 선정된 사용자는 Chrome 브라우저를 시작할 때 화면에서 참여 동의를 요청하는 알림을 받음

  - 사용자가 이에 대한 동의를 거부하더라도 Chrome 웹 탐색에는 아무런 영향을 미치지 않음

  - 만약 초기에 실험 참여에 동의를 제공한 사용자가 동의를 철회하고자 하는 경우, Chrome 브라우저 설정의 '개인정보 및 보안' 탭에서 '프라이버시 샌드박스' 탭으로 이동하여 선택 재고가 가능

- **(서드파티 쿠키 차단)** 프라이버시 샌드박스 활성화로 인해 서드파티 쿠키가 즉시 차단되지는 않으나, 직접 서드파티 쿠키를 차단하고자 하는 사용자는 Chrome 브라우저 설정의 '개인정보 및 보안' 탭에서 '쿠키 및 기타 사이트 데이터'를 선택해 차단이 가능

- **(웹퍼블리셔의 의무사항)** 위와 같이 사용자들이 서드파티 쿠키 차단 기능을 설정하더라도, 사용자 기기에 액세스하고자 하는 웹퍼블리셔들은 법적 의무를 준수해야 함

  - 웹퍼블리셔는 CNIL이 발행한 쿠키 지침[19]에 명시된 조건에 따라 사용자의 동의를 반드시 획득해야 함

  - 또한 웹퍼블리셔는 웹사이트에서 서드파티 쿠키를 대체(또는 함께 병행)하는 추적 장치를 사용하고 있다는 정보를 사용자들에게 투명하게 제공해야 함

19) https://www.cnil.fr/fr/cookies-et-autres-traceurs/regles/cookies/lignes-directrices-modificatives-et-recommandation

▶ 한편 싱가포르의 정보통신미디어개발청(IMDA)은 아시아태평양 지역 개인정보 감독기관 중 최초로 싱가포르 기업들의 개인정보보호 중심 환경 조성을 지원하기 위해 Google과 파트너십을 체결('23.7.)

- 싱가포르 내 등록 기업은 '23년 8월부터 IMDA의 개인정보보호 강화기술(PET) 샌드박스 제도*를 통해 Google 프라이버시 샌드박스에 대한 액세스를 지원받을 예정

* IMDA는 '22년 7월 싱가포르 개인정보보호 위원회(PDPC)와 공동으로 PET 샌드박스 제도를 개시하여 개인정보 활용 가치를 제고하고 개인정보 공유에 따른 산업계의 우려사항을 해소하고자 함

- IMDA와 Google의 협동 프로젝트인 'IMDA-Google: PET x Privacy Sandbox'[20]는 애드테크 전문가, 웹 운영자 및 개발자 등을 대상으로 설계

  - 동 파트너십은 싱가포르 현지 기업들이 고객 개인정보와 같은 민감한 정보를 손상시키지 않고 데이터를 활용하거나 공유할 수 있는 기회를 제공

3. 요약 및 시사점

▶ 사용자는 디지털 광고 생태계에서 자신의 개인정보가 어떻게 사용되는지 통제할 수 있는 권리가 그 어느 때보다 많아졌으며, 이러한 권리에 대한 인식도 점점 높아지고 있음

- 그간 애드테크(ad-tech) 업계에서는 서드파티 쿠키에 크게 의존해 맞춤형 광고를 제공해 왔기에, 서드파티 쿠키가 소멸될 경우 지금과 같이 강력한 행동기반 맞춤형 광고 제공이 어려워질 것으로 전망

- 전 세계적으로 개인정보보호 관련 규제가 빠르게 발전하고 있는 만큼, 기업들이 광고 목적으로 데이터를 활용함에 있어 법률을 준수하고 사용자들의 기대에 부응해야 할 필요성 또한 주목받고 있음

- 특히 투명성, 동의 및 개인정보 처리 의무를 준수할 필요성은 서드파티 쿠키의 퇴출 이후에도 이어질 것으로 예상

▶ 개인정보보호에 대한 규제 강화로 인해 제기되는 서드파티 쿠키의 제어 필요성으로 인해 광고업계와 웹퍼블리셔들에 있어 변화가 불가피할 전망

- (퍼블리셔) 잠재적인 광고주를 유치하는 데 자산이 될 수 있는 사용자들의 퍼스트파티 쿠키 데이터가 이미 확보되어 있기에, 변화에 대한 적응이 광고주들에 비해 상대적으로 수월할 수 있음

20) https://rsvp.withgoogle.com/events/privacysandbox-sg

- 다만, 소규모 퍼블리셔의 경우 개인정보 수집 및 보강을 강화할 수 있는 새로운 접근 방식을 테스트 할 수 있는 예산이 충분하지 않아 서드파티 쿠키의 퇴출에 충분히 대비하지 못하는 결과를 초래할 수 있음

• (광고주) 서드파티 쿠키 수집 및 사용의 제한으로 인해 소비자의 관심 파악이 어려워 광고 효율 하락에 직면하게 되므로, 지속적인 성공을 위해서는 프라이버시 샌드박스와 같은 대체 솔루션을 적극적으로 도입하는 노력이 요구

- Google의 프라이버시 샌드박스는 서드파트 쿠키를 혁신적인 개인정보보호 중심 솔루션으로 대체함으로써 디지털 광고 환경을 전환함과 동시에 개인정보보호에 대한 사용자의 우려를 해소할 잠재력을 보유

- 그러나 Google이 서드파티 쿠키 제공 중단 시기를 연이어 지연하고 있는 만큼, 프라이버시 샌드박스가 마케팅 업계에도 충분히 만족스러운 수준의 해답을 제공할 수 있을지에 대한 의문이 존재

Reference

1. 9to5google, Google delays when Chrome will phase out third-party cookies to 2024, 2022.7.27.
2. adpushup, Safari ITP: Intelligent Tracking Prevention Version 1.0 to 2.3, 2020.9.10.
3. CampaignAsia, Google forms privacy-first partnership with IMDa and advances Privacy Sandbox APIs, 2023.7.21.
4. CNIL, « Privacy Sandbox » sur Google Chrome : quelles conséquences pour les utilisateurs?, 2023.7.12.
5. Digiday, WTF is Apple's ITP 2.3 update?, 2019.9.27.
6. Euractiv, EU consumer department to present voluntary pledge over 'cookie fatigue', 2023.3.23.
7. Forbes, Apple ITP 2.1: What It Is, What It Means, And Why It Matters, 2019.4.10.
8. Google, The path forward with the Privacy Sandbox, 2022.2.11.
9. iab, A Guide to the Post Third-Party Cookie Era, 2022.3.
9. PartnerStack, Tracking, Cookies, and ITP 2.0, 2023.4.4.

EU-미국 데이터 프라이버시 프레임워크(DPF) 주요 내용 및 시사점

[목 차]

1. 개요 및 EU-미국 DPF의 추진 배경

(1) 개요

▶ EU 집행위원회(European Commission)는 EU와 미국 간 개인정보 이전을 위한 자체 인증 수단인 'EU-미국 데이터 프라이버시 프레임워크(이하 DPF)'[21]에 대한 적정성 결정을 채택('23.7.10.)

- 동 프레임워크 채택은 EU 사법재판소(Court of Justice of the European Union, 이하 CJEU)가 슈렘스 II(Schrems II)[22] 판결에서 기존 인증 수단이었던 'EU-미국 프라이버시 쉴드(Privacy Shield)' 협약을 무효화한 이래 3년이 지나 이루어짐

▶ EU 일반개인정보보호법(General Data Protection Regulation, 이하 GDPR) 제V장은 '적절한 수준의 보호'가 보장되거나 '적절한 안전장치'가 마련되어 있는 경우에만 EU 정보주체의 개인정보를 유럽경제지역(EEA)* 역외로 이전할 수 있다고 규정

* European Economic Area: 유럽의 양대 무역 블록인 유럽연합(EU)과 유럽자유무역연합(EFTA)을 합친 유럽 단일 통합 시장. 1994년 1월 1일에 EFTA와 EU 협정을 맺어 탄생

21) EU-US Data Privacy Framework

22) CJEU, Judgment of the Court (Grand Chamber) Data Protection Comissioner v. Facebook Ireland Limited, Maxilimillian Schrems (C-311/18), '20.7.16.

- 제3국에서 적절한 수준의 개인정보 보호가 보장되는 경우, EU 집행위원회는 GDPR 제45조에 근거해 적정성 결정을 내릴 수 있으며, 적정성 결정의 범위에 포함되는 모든 개인정보 이전은 추가적인 법적 보호 조치 없이 허용

- 이로써 DPF를 근거로 EU 시민의 개인정보를 EU에서 미국으로 이전할 경우, 표준계약조항(Standard Contractual Clauses, 이하 SCC)* 또는 구속력 있는 기업 규칙(Binding Corporate Rules, 이하 BCR)**과 같은 다른 이전 메커니즘에 의존할 필요가 없으며, 이전 영향 평가(Transfer Impact Assessment)를 수행할 필요 또한 없어짐

* 기업이 미국으로 데이터를 전송할 때 사용할 수 있는 규제 수단으로 '10년에 도입되었으며, '20년 CJEU의 슈렘스II 결정에 따라 '21년 개정됨

** 단일 또는 복수의 제3국에 위치한 컨트롤러(또는 프로세서)에게 개인정보를 이전하기 위해, 유럽연합 회원국 영토에 설립된 컨트롤러(또는 프로세서)가 준수하는 개인정보 정책(기업 내부 규칙). 기업이 내부 규칙으로 BCR을 설정하여 EU 내 소관 감독기관의 승인을 얻으면, 개별적 승인 절차없이 개인정보 국외 이전이 허용됨. 이 경우 컨트롤러(또는 프로세서)에게는 BCR 수립과 승인에 상당한 재정적 비용과 시간이 소요됨

(2) 추진 배경

▶ '95년 제정된 EU 개인정보보호지침(European Data Directive, Directive 95/46/EC)은 EU가 요구하는 수준에 부합하는 개인정보 보호가 보장되는 경우에만 개인정보를 EU 역외 국가로 이전할 수 있음을 명시

- 특히 EU는 미국의 법률이 EU 수준의 개인정보 보호 규제 체계를 갖추고 있는 것으로 간주하지 않아, 미국 기업들이 EU에서 자국으로 개인정보를 이전하고자 할 때, SCC와 같이 개별적으로 인증을 획득하는 절차를 요구

▶ 이에 EU 집행위원회는 개인정보보호 원칙을 준수하고 미국 정부의 인증을 받은 미국의 기업들이 EU에서 개인정보를 이전받을 수 있도록 '00년 7월 세이프하버(Safe Harbor)* 협약을 승인

* EU와 미국 간 개인정보 이전이 EU 개인정보보호지침에 따라 적절한 보호 수준을 보장하기 위해 마련된 자율 규제 프레임워크로, 미국 연방거래위원회(Federal Trade Commission, 이하 FTC)의 집행 권한으로 뒷받침

- 그러나 CJEU는 슈렘스Ⅰ 판결[23]을 통해 EU 집행위원회의 결정을 무효화 판결('15.10.6.)

  - 이는 ▲세이프하버 원칙이 자체 인증 시스템에 가입한 미국 기업에만 적용되며 미국 정부기관에게는 적용되지 않는다는 점 ▲미국의 국가 안보, 공익 및 법 집행과 상충하는 경우 세이프하버 협약보다 전자를 우선시하는 점을 근거로 함

23) CJEU, Judgment of the Court (Grand Chamber) Schrems v Data Protection Commissioner (C-362/14), '15.10.6.

▶ 세이프하버 무효화 이후 '16년 2월 2일, EU 집행위원회와 미국 상무부는 상업적 목적의 대서양 횡단 개인정보 이전을 위한 새로운 프레임워크인 EU-미국 프라이버시 쉴드에 합의

- EU-미국 프라이버시 쉴드는 '13년 11월의 EU 집행위원회 권고사항과 '15년 10월 CJEU가 기존 세이프하버 협약을 무효화한 판결에서 명시한 요건을 보완하여 마련
- 그러나 CJEU는 슈렘스 II 판결에서 ▲미국의 국가안보 관련 법*이 정보기관의 광범위한 감시를 허용하고 있으며 ▲프라이버시 쉴드의 옴부즈만 메커니즘에 정보기관을 구속할 수 있는 결정 권한이 없기에 EU 정보주체가 법적 구제를 받기 어렵다는 점을 근거로 프라이버시 쉴드와 관련된 적정성 결정을 무효화('20.7.16.)

* 대표적으로 ▲미국 국외정보감시법(FISA) 제702조[24] ▲행정명령 12333 (Executive Order 12333) ▲대통령 정책지시서 제28호 (Presidential Policy Directive 28) 등이 존재

▶ 세이프하버 협정 및 프라이버시 쉴드의 무효화로 인해 미국 기업들의 EU 개인정보 이전 번거로움이 지속적으로 발생하자, 미국 바이든 대통령은 앞의 두 CJEU 결정에서 제기되어온 우려 사항을 해결하고 개인정보보호 및 시민 자유 보호를 강화하는 행정명령(Executive Order 14086)에 서명[25]

- EU 집행위원회는 '22년 12월 동 프레임워크에 대한 적정성 결정 초안 공개 및 채택 절차 개시를 공지
- 이후 EU 집행위원회가 DPF에 대한 적정성 결정을 채택함에 따라 '23년 7월 10일부로 DPF의 효력이 발생

그림 _ EU-미국 간 개인정보 이전 규제 추진 경과('23.8.25. 기준)

24) 미국 정보기관이 국가 안보 목적으로 미국 역외에서 영장 없이 외국인의 통신정보를 수집, 분석 및 적절하게 공유할 수 있는 권한을 부여하는 조항

25) White House, Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities, '22.10.7. (https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/)

2. EU-미국 DPF 주요 내용[26)]

▶ **(개요)** CJEU의 우려사항을 해소하고 더욱 강력한 개인정보보호 수준을 보장하고자 DPF는 다음과 같은 주요 안전장치를 내포

- (정보 접근권한 제한) 미국 정보기관의 EU 개인정보에 대한 접근을 국가 안보 보호에 필요하고 비례적인(necessary and proportionate)' 범위로 제한
- (2단계 법적 구제 시스템) 미국은 EU 시민의 법적 구제를 위해 정부기관 내 담당부서를 지정하고, 전담 법원을 설치
  - (EU 시민의 권리 보호 및 민원 처리) 미국 정보기관의 정보접근에 대한 EU 정보주체의 권리 보장에 대하여 조사 및 민원 처리를 국가정보장실(ODNI)* 산하 '시민자유 보호 책임관(이하 CLPO)'**이 맡도록 함

* Office of Director of National Intelligence: 9.11 테러 이후 미국 정보공동체(CIA, FBI, NSA 등 미국 내 17개 정보기관을 통틀어 일컬음)의 공조, 총괄 관리 및 감독의 필요성 대두로 탄생한 국가정보장(DNI)을 보좌하는 기관으로 백악관 외부 독립기관이자 대통령의 직속기관. '05년 4월 설립

** Civil Liberties Protection Officer: '05년 ODNI이 설립된 이후 그 해 연말에 내부에 마련한 직책으로 미국 정보기관으로부터의 시민 자유 보호를 감시하고 민원을 처리

  - (소송 담당 법원) ▲정보기관 등이 CLPO의 결정에 불복할 경우, '개인정보보호 검토법원(Data Protection Review Court, 이하 DPRC)'에 소송을 제기할 수 있도록 하며, DPRC는 해당 소송에 대해 독립적으로 검토
- (EU 정보주체 권리 강화) 미국 기업이 개인정보를 잘못된 방식 또는 불법적으로 처리하는 경우, 정보주체에게 본인의 개인정보에 접근, 정정 또는 삭제할 수 있는 권한을 비롯해 GDPR에서 규정한 권리와 유사한 권리들을 부여
- (개인정보보호 원칙) DPF는 목적 제한, 개인정보 최소화, 보안, 개인정보 정확성, 투명성, 이전 제한 등 GDPR의 기본 원칙과 유사한 의무 원칙들을 명시

▶ **(자격 요건)** DPF를 통해 개인정보를 EU 컨트롤러 및 프로세서로부터 자유로이 이전받을 수 있는 기업은 DPF 인증을 획득한 조직에 한함

- DPF 참여 자격을 획득하기 위한 조건으로 조직은 미국 연방거래위원회(FTC) 또는 미국 교통부(Department of Transportation, 이하 DoT)의 조사 및 집행 권한에 속하는 조직이어야 함
  - 다만, EU 집행위원회가 발표한 적정성 결정에 따르면 은행, 보험사, 및 통신사 등의 경우 FTC와 DoT의 관할권 아래에 있지 않으므로 DPF에 참여할 수 없음

26) https://www.dataprivacyframework.gov/s/ 참고

▶ **(자체 인증)** DPF는 세이프하버 및 프라이버시 쉴드의 자체 인증 시스템을 유지하며, 이는 기업이 규정된 일련의 원칙을 준수하고 있음을 공개적으로 인증하거나 알리는 경우 미국에서 EU 개인정보를 전송받을 수 있음을 의미

- 과거 프라이버시 쉴드에 참여하지 않았던 조직은 인증을 획득하기 위해 미국 상무부(Department of Commerce, DoC)에 다음과 같은 정보를 제출해야 함
  - ▲조직의 이름 ▲개인정보 처리 목적에 대한 설명 ▲인증 대상이 될 개인정보 ▲검증 방법 ▲관련 독립적인 구제 메커니즘 ▲원칙 준수를 강제할 관할권을 가진 법정 기관 등
  - 이와 같은 인증 정보를 수령한 DoC는 해당 조직을 온라인에 공개되는 DPF 목록(DPF List)[27]에 추가하며, 조직은 해당 목록에 등재된 시점으로부터 동시에 DPF의 적용을 받음
- DPF는 이미 프라이버시 쉴드 자체 인증을 받은 조직에 DPF 인증으로 전환을 위한 별도의 의무를 부여하지는 않음
  - 대신 미국 국제무역청(International Trade Administration, 이하 ITA)은 이러한 조직에 자사 개인정보 처리 방침이 DPF 원칙에 부합하도록 10월 10일까지 업데이트할 것을 권고('23.7.11.)
- 한편 DPF를 근거로 계속 개인정보를 이전하고자 하는 조직들은 매년 DPF에 대한 참여를 재인증해야 함
  - 앞서 DoC는 매년 DPF의 자체 인증 및 재인증 절차가 실질적으로 동일하게 유지될 것이라고 명시한 바 있음

▶ **(주요 원칙)** DPF는 <제2장 원칙>(Ⅱ. Principles)과 <제3장 보충 원칙>(Ⅲ. Supplemental Principles)에서 개인정보 이전을 위한 신뢰성 있는 메커니즘을 제공하고 EU 정보 주체를 보호하기 위해 DPF에 참여하는 조직이 준수해야 할 주요 원칙들을 소개

- DPF에 참여하는 조직은 다음 표에서 소개하고 있는 개인정보보호 원칙을 준수해야 함

※ 이 중 ▲목적 제한 ▲개인정보 최소화 ▲개인정보 보안 ▲제3자와의 개인정보 공유에 대한 원칙은 프라이버시 쉴드의 원칙과 매우 유사

27) https://www.dataprivacyframework.gov/s/participant-search 참고

표 _ EU-미국 DPF 주요 원칙

원칙	주요 내용
목적 제한	• 개인정보는 처리 목적과 관련된 정보로 제한되어야 하며, 조직은 개인정보를 초기 수집한 목적이나 이후 정보주체가 승인한 목적과 양립할 수 없는 방식으로 개인정보를 처리해서는 안 됨 • 만약 초기 목적과 호환되는 새로운(변경된) 목적으로 개인정보를 사용하거나 제3자에게 공개하기 전, 조직은 ▲명확하고 ▲확실하며 ▲쉽게 이용할 수 있는 메커니즘을 통해 정보주체가 반대(옵트아웃)할 수 있는 기회를 제공해야 함
특수한 개인정보	• 조직은 민감정보를 ▲처음 수집한 목적 또는 이후 정보주체가 승인한 목적 이외의 목적으로 사용하거나 ▲제3자에게 공개하기에 앞서 정보주체로부터 명시적 동의를 받아야 함
개인정보의 정확성, 최소화 및 보안	• 개인정보는 정확해야 하며 필요한 경우 최신 상태로 유지되어야 함 • 또한 처리 목적과 관련하여 적절하고, 관련성 있으며 과도하지 않아야 하며, 원칙적으로 개인정보의 처리 목적에 필요한 기간보다 더 오래 보관하지 않아야 함 • 개인정보는 처음 수집 목적에 부합하거나 정보주체가 추후 승인한 목적에 부합하는 경우에만 개인을 식별할 수 있는 형태로 보관될 수 있음 • 개인정보는 무단 또는 불법 처리로부터 보호받고, 우발적인 손실, 파기 또는 손상으로부터 보호하는 등 보안을 보장하는 방식으로 처리되어야 함
투명성	• 조직은 정보주체에게 ▲조직의 DPF 참여 여부 ▲수집된 개인정보 유형 ▲처리 목적 ▲개인정보를 공개할 수 있는 제3자의 유형, 신원 및 목적 ▲정보주체의 권리 ▲조직에 연락할 수 있는 방법 ▲이용 가능한 구제수단 등을 알려야 함 • 개인에게 개인정보 제공을 처음 수집 목적과 실질적으로 다른 목적으로 사용되기 전, 또는 제3자에게 공개되기 전에 조직은 이러한 정보를 최대한 신속히 명확하고 확실하며 이해하기 쉬운 언어로 정보주체에게 통지해야 함
정보주체 권리	• 정보주체는 ▲본인의 개인정보 처리와 관련된 정보를 제공받을 권리 ▲부정확한 개인정보의 정정 및 삭제를 요청할 권리 ▲수집 목적과 다른 목적의 개인정보 처리 및 제3자 제공에 반대할 권리 등을 보유
개인정보의 추가 이전	• EU에서 미국 내 조직으로 전송된 개인정보의 보호 수준은 미국 또는 다른 제3국의 수신자에게 추가로 전송됨으로서 훼손되어서는 안됨
책임	• 개인정보를 처리하는 조직은 개인정보 보호 의무를 효과적으로 준수하기 위하여 적절한 기술적 및 조직적 조치를 취해야 하며, 특히 관할 감독 기관에 이러한 준수 사항을 입증할 수 있어야 함

▶ **(컴플라이언스)** DoC는 다양한 메커니즘을 통해 조직이 DPF 원칙을 효과적으로 준수하는지를 지속적으로 모니터링 할 예정

- 특히 무작위로 선정된 조직에 대한 불시 점검(spot checks)와 잠재적인 규정 준수 문제가 확인되는 경우 특정 조직에 대한 임시 현장 점검을 실시하여 다음 사항을 확인
  - 정보주체의 민원 및 요청을 처리하기 위한 연락 창구가 이용 가능한지
  - 조직의 개인정보 처리방침을 웹사이트와 DoC 웹사이트를 통해 쉽게 이용 가능한지
  - 조직의 개인정보 처리방침이 인증 요건을 지속적으로 준수하는지
  - 조직이 선택한 분쟁 조정 메커니즘을 통해 불만 처리가 가능한지
- 만약 모니터링 결과 조직이 지속적으로 DPF 원칙을 준수하지 않는 것으로 확인되는 경우 해당 조직은 DPF 목록에서 제거되며, 조직은 DPF를 통해 수신한 모든 개인정보를 반환하거나 삭제해야 함

▶ **(탈퇴)** DPF 탈퇴 시 조직은 사전에 DoC에 탈퇴 의사를 고지해야 하며, 그동안 DPF에 의거하여 수집한 개인정보에 대한 처리 방침(유지, 반환 또는 삭제 등)에 대해서도 언급해야 함

- 조직은 DPF 탈퇴 시 EU 지역으로부터 전송받은 개인정보를 반환 또는 삭제해야 하나, 다음과 같은 조치가 가능한 경우 예외적으로 개인정보 보관이 가능
  - 조직이 보관 예정인 개인정보에 대해 계속하여 개인정보 보호에 대한 원칙을 적용하겠다는 내용의 연례 업데이트를 DoC에 제출하는 경우
  - EU 집행위원회가 채택한 SCC의 요구 사항을 완전히 반영하는 계약의 사용 등 기타 승인된 수단을 통해 개인정보에 대한 '적절한' 정보 보호를 제공할 수 있는 경우
- 또한 DPF에서 탈퇴하는 조직은 자사 개인정보 처리방침에서 DPF에 참여한다거나 그로 인한 혜택을 받을 자격이 있음을 암시할만한 DPF에 대한 모든 언급을 삭제해야 함

▶ **(피해 구제 체계)** DPF는 EU의 정보주체가 본인의 권리 행사를 위해 ▲해당 조직 ▲조직이 지정한 분쟁조정기관 ▲국가 개인정보 감독기관(DPA) ▲DoC ▲FTC를 통해 규정 미준수에 대해 민원을 제기하고 관련 문제를 해결할 수 있는 가능성을 제공

- (조직을 통한 구제) 조직은 정보주체의 민원을 처리하기 위한 효과적인 구제 메커니즘을 마련해야 함
  - 조직은 개인정보 처리방침을 통해 민원을 담당·처리할 조직 내부 또는 외부의 연락 창구를 정보주체에게 명확하게 알려야 함

- 정보주체로부터 직접, 또는 정보주체로부터 민원을 신고 받은 EU 회원국의 DPA로부터 사안을 회부받은 DoC를 통해 민원을 접수한 조직은 45일 이내에 해당 민원에 대응해야 함

- (조직 지정 분쟁조정 기관) 정보주체는 해당 조직이 지정한 분쟁조정 기관에 직접 민원을 제기하여 무료로 적절한 구제책을 제공받을 수 있음

  - 이러한 기관이 부과하는 제재 및 구제책은 조직의 원칙 준수를 보장할 수 있을 만큼 충분히 엄격해야 하며, 문제가 되는 개인정보의 추가 처리 중단 및/또는 삭제 등을 제공해야 함

- (DPA) 정보주체는 해당 국가의 개인정보 감독기관(DPA)에 민원을 제기할 수 있으며, 조직은 해당 사안에 대한 DPA의 조사에 적극적으로 협조할 의무가 있음

  - 만약 DPA가 제공한 권고사항을 조직이 준수하지 않을 경우, DPA는 ▲해당 조직을 DPF 목록에서 삭제할 권한이 있는 DoC, 또는 ▲DPA에 협조하지 않거나 원칙 미준수 조직에 대해 미국 법률에 의거해 조치할 수 있는 FTC 및 DoT에 해당 사건을 회부할 수 있음

- (DoC) DoC가 조직의 원칙 미준수에 대한 민원을 접수하는 경우, DoC는 DPA가 민원을 조직의 연락 담당자에게 전달하고 조직과의 후속 조치를 통해 해결을 촉진할 수 있는 특별 절차를 제공

- (FTC) FTC는 DoC 및 DPA로부터 접수된 DPF 원칙 미준수 건에 대해 우선적으로 고려하여 FTC법 제5조 위반 여부를 결정

  - 또한 FTC는 영향을 입은 정보주체로부터 직접 민원내용을 접수하고 특히 개인정보 보호 문제에 대한 광범위한 조사의 일환으로 자체적인 조사를 수행할 수 있음

  - FTC는 임시·영구 금지 명령 또는 기타 구제책에 대한 행정 또는 연방 법원 명령을 제공할 수 있으며, 조직이 이러한 명령을 준수하지 않을 경우 FTC는 민사 처벌 또는 기타 구제 조치를 취할 수 있음

- 이 외에도 조직이 DPF 원칙 준수 및 공개된 개인정보 처리방침 준수 의무를 지키지 못한 경우, 정보주체는 불법행위법(Tort Law), 소비자법 등 미국 법률을 근거로 손해배상을 포함한 사법적 구제 수단을 추가로 이용할 수 있음

- (정보기관 수집 관련 구제) 한편 DPF는 국가 안보와 관련한 미국 정보기관의 정보접근과 관련하여 미국으로 이전된 EU 정보주체의 민원을 해결하기 위해 2단계 메커니즘을 구축

- 민원 제기가 인정받기 위해 EU 정보주체는 본인의 개인정보가 실제로 미국 조직에 의해 수집되었다는 사실을 별도로 입증할 필요가 없음
- (1단계) 정보주체는 DPA에게 직접 민원을 제기할 수 있으며, 해당 민원은 EU 개인정보보호이사회(EDPB)에 의해 미국으로 전송되어 CLPO가 조사에 착수
- (2단계) CLPO의 결정에 불복한 정보주체는 DPRC에 소송을 제기할 권리가 있음

3. 시사점 및 평가

▶ **(시사점)** EU 집행위원회의 이번 DPF 적정성 결정 채택은 EU 역내 시민의 개인정보에 대해 미국이 적절한 수준의 보호를 보장한다고 공식적으로 인정했음을 의미하는 점에서 시사하는 바가 큼

- 동 적정성 결정 채택을 계기로 미국으로 개인정보를 이전하고자 하는 기업들은 SCC나 BCR 등 기타 이전 메커니즘에 비해 덜 번거롭고 덜 복잡한 대안 선택이 가능
- 이번 DPF에 관한 협약은 EU와 미국 간의 경제 협력 촉진 및 EU 시민의 개인정보 보호를 강화하는 데 기여할 것으로 기대

▶ **(비판)** 한편 세이프하버와 프라이버시 쉴드의 무효화를 이끌어낸 막스 슈렘스(Max Schrems) 변호사가 설립한 개인정보 보호 시민단체 NOYB*는 DPF가 세이프하버 협정이나 프라이버시 쉴드와 본질적인 차이가 없다고 지적

* NOYB(None of your business) – European Center for Digital Rights

- (NOYB) EU와 미국이 사용하는 '비례적'이라는 단어의 의미가 서로 다르며, 미국의 이해에 따라 미국 정보기관이 개인정보를 대량으로 모니터링을 하는 행위 자체를 비례적으로 판단하는 등 개념에 대한 합의가 제대로 이뤄지지 않음을 비판
  - NOYB는 미국 정보기관의 감시를 충분히 축소하거나 효과적인 법적 구제를 제공하기 위해서는 EU에서 허용하는 비례성 기준에 부합하는 수준으로 미국의 법률 개정이 요구되며, 이를 해결하지 못할 경우 DPF가 앞서 무효화된 규정들의 전철을 밟게 될 것이라고 경고
  - 그러나 미국은 미국인이 아닌 사람은 미국에서 헌법상 권리가 없으므로 개인정보 보호권 침해가 수정헌법 제4조에 적용되지 않는다고 주장하며 FISA 제702조의 개정을 거부 중
- (EDPB) 접근권에 대한 일부 면제, 주요 정의의 부재, 프로세서에 대한 DPF 원칙의 적용에 대한 명확성 부족, 공개적으로 접근할 수 있는 권리에 대한 광범위한 면제 등과 관련해 우려를 표출

- EDPB는 새로 도입된 필요성과 비례성 원칙의 적용과 관련하여 면밀한 모니터링이 필요하다는 점과, 개인정보의 임시 대량 수집과 함께 대량으로 수집된 개인정보의 추가 보존 및 배포에 관해서도 더 명확한 설명이 필요하다는 입장

- 개인정보 이전으로 인해 보호 수준이 훼손되어서는 안 되기 때문에, 최초 수령자가 제3국 수입업자에게 부과한 보호 조치가 이후 이전에 앞서 제3국 법률에 따라 효과적이어야 한다는 점을 명확히 할 필요가 있음을 제기

• (기타) 이밖에 개인정보 보호와 비즈니스 운영 간의 균형 유지에 대한 어려움, 즉 DPF의 효율성 부족 및 복잡성으로 인한 비용 증가 문제도 고려해 볼 사안

▶ **(향후 전망)** 이번 EU-미국 DPF 유효성이 CJEU로부터 무효화될 여지가 남아 있으며, 영국-미국 및 스위스-미국의 DPF 체결에도 영향을 끼칠 전망

• (유효성에 대한 불안 요소) NOYB가 다시 한 번 CJEU에 DPF 무효화를 위한 의견을 제기할 가능성이 매우 높으므로 이번에 체결된 EU-미국 DPB 역시 유효성에 타격을 입을 소지가 존재하는 점은 불안 요소로 작용

• (영국으로의 EU-미국 DPF 확장) EU와 미국 간 DPF에 대한 EU 집행위원회의 적정성 결정 채택은 영국과 미국 간의 개인정보 흐름을 촉진하는 데이터 프라이버시 프레임워크(DPF) 도입의 발판을 마련[28]

- 미국과 영국 간 DPF가 도입되기 위해서는 미국이 영국을 '적격 국가(qualifying state)'로 지정하고 영국 국무장관이 적정성 결정을 내려야 함[29]

• (스위스-미국 간 DPF) 또한 '23년 7월 17일부로 스위스와 미국 간의 DPF도 시행되었으며, 기존 스위스-미국 프라이버시 쉴드에 따라 인증을 받은 기관은 새로운 DPF로 원활하게 전환이 가능[30]

- 다만 영국과 마찬가지로 스위스가 적정성 결정을 내릴 때까지는 개인정보 이전을 할 수 없음

28) UK EXTENSION TO THE EU-U.S. DATA PRIVACY FRAMEWORK
https://www.dataprivacyframework.gov/s/framework-text?tabset-c1491=2
29) FAQs - UK Extension to the EU-U.S. Data Privacy Framework (UK Extension to the EU-U.S. DPF)
https://www.dataprivacyframework.gov/s/article/FAQs-UK-Extension-to-the-EU-U-S-Data-Privacy-Framework-UK-Extension-to-the-EU-U-S-DPF-dpf
30) SWISS-U.S. DATA PRIVACY FRAMEWORK
https://www.dataprivacyframework.gov/s/framework-text?tabset-c1491=3

Reference

1. Dataguidance, International: Commission adopts adequacy decision on EU-US DPF - what you need to know, 2023.7.13.
2. Dataguidance, The Definitive Guide to Schrems II, 2022.11.22.
3. EDPB, FTC EDPB welcomes improvements under the EU-U.S. Data Privacy Framework, but concerns remain, 2023.2.28.
4. European Commission, Adequacy decision for the EU-US Data Privacy Framework, 2023.7.10.
5. European Commission, Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows, 2023.7.10.
6. European Commission, EU-U.S. Privacy Shield: Frequently Asked Questions, 2023.7.12.
7. European Commission, Questions & Answers: EU-US Data Privacy Framework, 2023.7.10.
8. European Law Blog, Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for data protection authorities, 2015.10.15.
9. IAPP, EU-US Data Privacy Framework adopted, what now?, 2023.7.24.
10. JDSUPRA, Certification Under the EU-U.S. Data Privacy Framework, 2023.7.19.
11. Loyens & Loeff, EU-US Data Privacy Framework adopted by the European Commission (Third time's a charm?), 2023.7.18.
12. noyb, European Commission gives EU-US data transfers third round at CJEU, 2023.7.10.
13. Techcrunch, Europe's Top Court Strikes Down 'Safe Harbor' Data-Transfer Agreement With U.S., 2015.10.6.
14. The White House, FACT SHEET: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework, 2022.10.7.
15. The White House, United States and European Commission Joint Statement on Trans-Atlantic Data Privacy Framework, 2022.3.25.

<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

2023

개인정보보호 월간동향분석 제8호

발 행 2023년 9월 6일

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

1. 본 보고서는 개인정보보호위원회 「개인정보보호 동향 분석」 사업 수행 결과물입니다.
2. 본 보고서의 저작권은 한국인터넷진흥원에 있으며, 본 보고서를 활용하실 경우에는 출처를 반드시 밝혀주시기 바랍니다.
3. 본 보고서의 내용은 한국인터넷진흥원의 공식 입장과는 다를 수 있습니다.