2024 Privacy Report

개인정보보호 월간동향분석

1월호

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2024 Privacy Report

개인정보보호 월간동향분석

1월호

1. EU 데이터법(Data Act)주요 내용 분석 및 시사점

2. EU 내 메타의 무광고 유로 서비스 모델의 개인정보 침해 이슈 분석

KISA

EU 데이터법(Data Act) 주요 내용 분석 및 시사점

[목 차]

1. 개요

2. 주요 내용
(1) 적용 범위
(2) 제품 제조자 및 관련 서비스 제공자 의무사항
(3) 사용자 권리 및 데이터 보유자 의무사항
(4) 클라우드 전환
(5) 감독 및 과징금

3. 데이터법과 GDPR의 관계성

4. 결론 및 시사점

1. 개요

▶ **(개요)** '데이터법(Data Act)'[1]이 '23년 12월 EU 관보(Official Journal of the European Union) 게재 후 '24년 1월 11일부터 공식 발효됨에 따라, 20개월간의 유예기간을 거쳐 '25년 9월부터 EU 전역에서 시행 예정

- 데이터법의 제정은 ▲데이터에 대한 접근 촉진 ▲데이터 가치 창출에 대한 투자 장려 ▲데이터 처리 서비스 제공자 간의 전환 활성화 ▲불법 데이터 유통에 대한 안전장치 마련 ▲부문 간 데이터 재사용을 위한 상호운용성 표준 개발 등을 목표로 함

1) 정식 명칭은 '데이터에 대한 공정한 접근 및 사용에 관한 조화로운 규칙에 관한 규정 (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828)'

▶ **(도입 배경)** 동법은 EU 집행위원회가 '20년에 수립한 'EU 데이터 전략(a European Strategy for Data)'*의 구현을 위해 데이터 거버넌스법(DGA, Data Governance Act)**에 이어 두 번째로 제정한 법률[2)]

* 동 전략은 EU 집행위원회가 제시한 6대 주요 정책 추진 전략 중 하나인 '디지털 시대에 부합한 유럽(a Europe fit for the Digital Age)'의 일환. '30년까지 국제경쟁력과 데이터 주권(data sovereignty)을 보장하는 EU 단일 데이터 시장의 조성을 목표로 함.

** '22년 6월 제정되어 '23년 9월 전면 시행된 데이터 거버넌스법은 개인정보와 非개인정보를 모두 포괄하며, 기업이 고품질 산업 데이터에 쉽게 접근하여 성장을 가속화하고 가치를 창출할 수 있는 기반을 마련

- 데이터 거버넌스법이 기업, 개인, 공공부문의 자발적인 데이터 공유를 촉진하기 위한 구조 및 절차를 정립하는 반면*, 데이터법은 데이터의 접근과 사용을 규제하여 어떤 주체가 어떠한 조건에서 데이터로 가치를 창출할 수 있는지 명확히 함으로써 데이터 거버넌스법을 보완

  * 공공데이터의 재사용, 데이터 중개자(data intermediaries) 또는 데이터 이타주이(data altruism) 규제에 중점을 두고 있음

▶ **(구성체계)** 데이터법은 총 11장 50개 조항으로 구성

표 1_ 데이터법의 구성

장		조항	주요 내용
1장	총칙	제1조~제2조	▪ 적용 범위, 주요 용어 정의
2장	B2B 및 B2C 데이터 공유	제3조~제7조	▪ 제품 또는 관련 서비스 사용으로 생성된 데이터의 공유와 관련된 의무 및 권리 보장
3장	데이터 보유자의 데이터 제공 의무	제8조~제12조	▪ 데이터 보유자가 데이터 수취인에게 데이터를 제공해야 하는 의무 및 보상 조건
4장	기업 간 데이터 접근 및 사용과 관련된 불공정약관	제13조	▪ 불공정한 내용의 데이터 공유 약관 조항의 사용 금지
5장	예외적 필요에 따른 공공기관, EU 집행위원회, 유럽중앙은행 및 기타 EU 기관의 데이터 접근	제14조~제22조	▪ 비상사태 및 공익 등 예외적 상황에 한한 공공기관의 데이터 접근 허용
6장	데이터 처리 서비스 간 전환	제23조~제31조	▪ 클라우드 서비스 전환과 관련된 데이터 처리 서비스 계약 세부사항 및 제한
7장	국제 및 제3국 정부의 무단 접근 및 非개인정보의 역외이전	제32조	▪ EU 역내 非개인정보에 대한 무단 접근 방지 및 지식재산권·영업비밀 보호 보장
8장	상호운용성	제33조~제36조	▪ 데이터 및 데이터 서비스의 상호운용성 촉진을 위한 의무사항, 데이터 공유 목적의 스마트계약 사용

2) European Commission, A European Strategy for data, 2024.1.12.
3) 정식 명칭은 '데이터베이스의 법적 보호에 관한 1996년 3월 11일 유럽 의회 및 이사회의 지침(Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases)'

9장	이행 및 집행	제37조~제42조	▪ EU 회원국이 지정한 국가 규제기관의 법 이행 및 집행 의무, 피해구제체계, 위반에 대한 과징금
10장	지침 96/9/EC[3]에 따른 특별권(*Sui Generis* Right)[4]	제43조	▪ 특별권은 제품 또는 관련 서비스의 사용을 통해 생성된 데이터베이스에 적용되지 않음
11장	최종규정	제44조~제50조	▪ 기타 EU 법률과의 관계 등

출처: 데이터법(2023), 넥스텔리전스(주) 재구성

2. 주요 내용

(1) 적용 범위

▶ 데이터법은 컨넥티드 제품(이하 제품)*을 통해 그 구성 요소와 관련된 서비스** 제공 과정에서 수집한 개인정보 및 非개인정보(예: 산업 데이터)를 모두 포괄

* connected product: 사용 또는 환경에 관한 데이터를 수집 또는 생성하고 제품 정보를 전달할 수 있는 제품

** related service: 제품에 통합되거나 연결된 소프트웨어를 포함한 디지털 서비스

- 사용자 인터페이스 및 기기 자체에서 생성된 원시 데이터(raw data)는 적용 대상에 포함되나, 이러한 데이터에서 추론되거나 파생된 정보는 적용 대상에서 제외
- 또한, 사용자가 콘텐츠를 기록, 전송, 표시 또는 재생하는 동안 센서가 장착된 제품이 생성하는 데이터와 데이터 공유 관련 콘텐츠도 적용 대상이 아님

▶ 데이터법은 역외 적용이 가능하며, 규율 대상은 다음과 같음

- EU 시장에 출시된 제품 제조자 및 관련 서비스 제공자
- EU 역내에서 제품 또는 서비스를 이용해 데이터를 생성하는 사용자(user)

  ※ 사용자는 제품 또는 관련 서비스를 소유하거나, 일시적으로 사용할 권리를 보유하거나, 관련 서비스를 제공받는 자연인 또는 법인. 사용자가 항상 데이터를 생성하지는 않으나, 데이터 보유자에 해당할 수도 있음
- EU 역내에서 데이터를 제공받는 제3자인 데이터 수취인(data recipient)
- EU 역내 데이터 수취인에게 데이터를 제공하는 데이터 보유자(data holder)

  ※ 데이터 보유자의 소재지와는 관계없이 적용
- EU 역내 고객에게 서비스를 제공하는 데이터 처리 서비스 제공자

  ※ 데이터 처리 서비스 제공자의 사업장 소재지와는 관계없이 적용

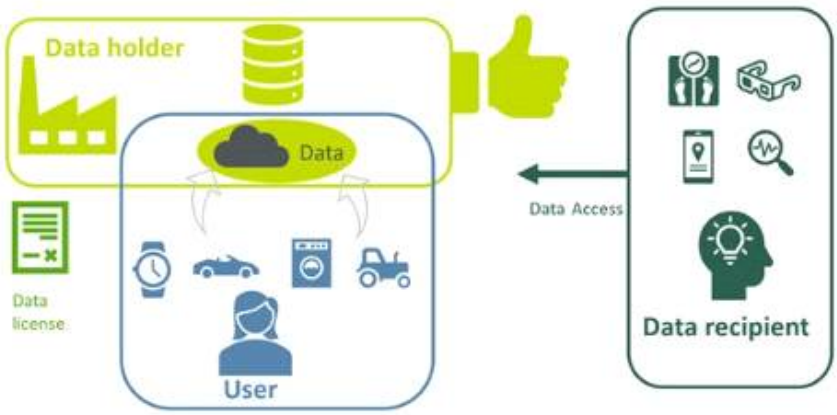
4) 지침 96/9/EC 제7조는 데이터베이스에 대한 실질적 투자를 인정하는 재산권인 특별권(*sui generis* right)의 존속기간을 규정하고 있으며, 이를 통해 데이터베이스 제작자는 데이터베이스 내용의 무단 추출하거나 재사용을 금지할 수 있음

- 규정에 따라 데이터에 접근하는 EU 기관* 및 공공기관

  * ▲EU 집행위원회 ▲유럽중앙은행 ▲기타 EU 기관

- 데이터스페이스(Data Space) 참여자, 스마트계약을 사용하는 애플리케이션 공급자 및 스마트계약 배포와 연관된 자

그림 _ 데이터법에 따른 이해관계자 상관관계



출처: Hogan Lovells(2023)[5]

▶ 데이터법에서 데이터 보유자에게 부과하는 데이터 공유 의무는 기업과 소비자 간 거래(B2C) 및 기업과 기업 간 거래(B2B) 사용자에게 적용

- 데이터 공유 권한은 B2C 및 B2B 사용자뿐만 아니라 예외적으로 기업 대 정부(B2G) 사용자에게도 부여

(2) 제품 제조자 및 관련 서비스 제공자 의무사항

▶ **(데이터 접근 중심 설계)** 제품 제조자와 관련 서비스 제공자는 기본적으로 사용자가 해당 제품 및 서비스 데이터에 무료로 쉽고 안전하게 직접 접근할 수 있도록 상품과 관련 서비스를 설계·제조·제공해야 함

- 이러한 데이터는 포괄적이고, 구조화되어있으며, 기계 판독이 가능한 형식이어야 함

▶ **(정보 제공)** 사용자와의 제품 구매, 대여 또는 임대 계약 체결에 앞서 제조업체는 사용자에게 명확하고 이해하기 쉬운 형식으로 특정 정보*를 제공해야 함

  * ▲제품이 생성할 수 있는 데이터 유형, 형식 및 양 ▲제품이 지속적·실시간으로 데이터를 생성할 수 있는지 여부 ▲데이터를 기기 내에 또는 원격으로 저장할 수 있는지 여부 및 보관기간 ▲사용자 데이터 액세스, 검색 또는 삭제 방법 등

5) Hogan Lovells(2023.12.7.), Deep Dive on the new EU Data Act, https://www.engage.hoganlovells.com/knowledgeservices/news/deep-dive-on-the-new-eu-data-act

- 관련 서비스 제공자 또한 서비스 공급 계약을 체결하기 전 사용자에게 유사한 정보를 제공해야 하며, 추가적으로 제공해야 하는 정보로는 ▲제3자의 데이터 사용 가능성 및 사용 목적 ▲사용자가 제3자에게 데이터 공유를 요청할 수 있는 방법 ▲사용자가 데이터 공유를 중단하거나 데이터법 위반에 대한 민원을 제기할 수 있는 방법 등이 있음

(3) 사용자 권리 및 데이터 보유자 의무사항

▶ **(데이터 접근권)** 사용자가 직접 데이터에 접근할 수 없는 경우, 데이터 보유자는 사용자 요청에 따라 지체없이 제품 또는 관련 서비스의 데이터에 대한 접근 권한을 사용자에게 제공해야 함

- 단, 데이터 보유자는 보안 목적 및 영업비밀 보호 등의 특정 조건 하에서 사용자의 데이터 접근을 제한할 수 있음

- (보안) 데이터에 대한 접근 제공이 인간의 건강과 안전 또는 제품의 보안 요건을 심각하게 훼손할 수 있는 경우 데이터 보유자는 데이터 접근, 사용 또는 공유를 제한·금지할 수 있음

  ※ 데이터 보유자는 데이터 공유 거부에 대해 관할 기관에 이를 통지해야 함

- (영업비밀) 또한 데이터법은 데이터를 경쟁 제품 개발에 활용하는 것을 금지하고 있으며, 데이터 보유자와 사용자가 기밀 유지를 위해 필요한 모든 기술적, 조직적 조치를 취한 경우에만 영업 비밀을 사용자에게 제공할 수 있음

▶ **(제3자 공유)** 데이터법은 사용자에게 데이터에 단순히 접근할 수 있는 권한 뿐 아니라 데이터 보유자에게 제3자(데이터 수취인)와 즉시 사용한 데이터를 공유하도록 요청할 수 있는 권리도 부여

- 사용자의 요청에 따라 데이터 보유자는 사용자와 동일한 방식으로 데이터 수취인에게 데이터를 공유할 의무가 있음

- 다만, ①아직 시장에 출시되지 않은 신제품과 연관된 즉시 사용 가능한 데이터의 공유 ②디지털시장법(Digital Markets Act)에서 규정한 게이트키퍼(gatekeeper)*와의 데이터 공유는 제한

  * 유럽에서 핵심 플랫폼 서비스를 제공하는 대형 디지털 플랫폼.

- B2B 관계에서 데이터 보유자가 데이터 수취인에게 데이터를 제공해야 하는 경우 제공 방식은 양 당사자 간에 체결한 계약을 통해 결정하며, 해당 계약은 불공정 약관을 포함하지 않아야 함

- 데이터 보유자는 데이터 수취인을 범주에 따라 차별해서는 안 되며, 사용자가 별도로 요청하지 않는 한 독점적으로 데이터를 수취인에게 제공해서는 안 됨
- 데이터 제공에 대해 데이터 보유자와 데이터 수취인 간에 합의된 모든 보상은 비차별적이고 합리적이어야 하며, 데이터 수취인이 중소기업 또는 비영리단체가 아닌 이상 보상금에는 매출이익(margin)이 포함될 수 있음

▶ **(공공부문과의 데이터 공유)** 자연재해와 같이 공익에 영향을 미치는 예외적인 상황일 경우, 민간 데이터 보유자는 EU 기관의 요청에 따라 데이터를 제공해야 함

- 이와 같은 요청은 요청기관이 동등한 조건에서 적시에 효과적인 방식으로 그러한 데이터를 얻을 수 있는 대체 수단이 부재한 경우에만 허용

(4) 클라우드 전환

▶ 클라우드 서비스 부문의 경쟁 축소를 방지하고자 데이터법은 사용자가 클라우드 서비스를 쉽게 전환할 수 있도록 규정

- 데이터 처리 서비스 계약은 전환 절차 착수를 위한 최대 통지 기간을 언급해야 하며, 해당 기간은 2개월을 초과할 수 없음
- 또한, 관련 서비스 제공자는 통지 기간 이후 30일 이내에 모든 데이터, 애플리케이션 및 디지털 자산이 새로운 서비스 제공자에게 이전될 수 있도록 보장해야 함
- 클라우드 전환 비용은 데이터법의 시행일로부터 3년간의 유예기간에만 청구할 수 있으며, 유예기간 종료 후에는 전환 비용 청구가 전면 금지될 예정

(5) 감독 및 과징금

▶ **(감독기관)** 데이터법의 이행과 집행을 보장하기 위해 EU 회원국은 하나 이상의 관할 감독기관을 지정해야 함

- 감독기관을 두 개 이상 지정한 경우, 대표 연락 창구가 될 데이터 코디네이터를 임명
- 관할 감독기관의 주요 담당 업무는 ▲위반 혐의에 대한 민원 조사 및 다른 관할 기관과의 협력 ▲과징금 등의 금전적 제재 부과 ▲데이터 제공 및 활용을 위한 기술 개발 모니터링 등을 포함

▶ **(과징금)** 각 회원국은 데이터법 위반자의 직전 회계연도의 EU 역내 연간 매출액을 비롯한 요소들을 고려하여 과징금을 정할 책임이 있음

- 특히 개인정보의 공유에 관한 조항을 위반한 경우, GDPR 과징금 조항에 근거하여 최대 2,000만 유로 또는 전 세계 연간 매출액의 4% 중 큰 금액을 부과

3. 데이터법과 GDPR의 관계성

▶ GDPR의 적용 범위가 개인정보로 제한되는 한편, 데이터법은 개인정보 및 非개인정보를 모두 포괄하는 데이터에 적용

▶ 그러나 데이터법은 GDPR에서 규정한 정보주체의 권리 및 개인정보 감독기관의 권한 등을 제한하지 않으며, 제품 또는 관련 서비스에서 개인정보가 생성되는 경우 데이터법 및 GDPR의 요건을 모두 충족해야 함

- 데이터법 제1조제5항은 데이터법의 적용을 받는 데이터가 개인정보인 경우 GDPR을 우선 적용한다고 명시

표 2_ 데이터법 제1조제5항

(원문)
This Regulation is without prejudice to Union and national law on the protection of personal data, privacy and confidentiality of communications and integrity of terminal equipment, which shall apply to personal data processed in connection with the rights and obligations laid down herein, in particular Regulation (EU) 2016/679 and (EU) 2018/1725 and Directive 2002/58/EC, including the powers and competences of supervisory authorities and the rights of data subjects. Insofar as users are data subjects, the rights laid down in Chapter II of this Regulation shall complement the rights of access by data subjects and rights to data portability under Article 15 and 20 of Regulation (EU) 2016/679. **In the event of a conflict between this Regulation and Union law on the protection of personal data or privacy, or national legislation adopted in accordance with such Union law, the relevant Union or national law on the protection of personal data or privacy shall prevail.**

(국문)
본 규정은 개인정보 보호, 통신의 프라이버시 및 기밀성, 단말기 장비의 무결성에 관한 EU법 및 EU 회원국의 국내법을 침해하지 않으며, 이는 여기에 명시된 권리와 의무, 특히 감독 당국의 권한과 권한 및 정보 주체의 권리를 포함하여 EU 규정 2016/679* 및 EU 규정 2018/1725, 지침 2002/58/EC와 관련하여 처리되는 개인정보에 적용된다. 사용자가 정보주체인 한, 본 규정의 제2장에 명시된 권리는 EU 규정 2016/679의 제15조 및 제20조에 따른 정보주체의 접근권 및 정보 이동권을 보완한다. **본 규정과 개인정보 또는 개인정보 보호에 관한 EU 법률 또는 해당 법률에 따라 채택된 국내법이 상충하는 경우, 개인정보 또는 개인정보 보호에 관한 관련 EU법 또는 국내법이 우선한다.**

* EU 일반 개인정보보호법(GDPR, General Data Protection Regulation)

- 데이터법 자체가 개인정보 처리의 법적 근거를 새로 마련하고 있지는 않기에, 일반적으로 개인정보의 처리는 GDPR 제6조(처리의 적법성) 및 제9조(특별 범주의 개인정보 처리)에서 명시한 요건을 준수해야 함

- 따라서 데이터 보유자는 제공하고자 하는 데이터가 개인정보에 해당하는지 식별해야 하며, 유효한 법적 근거가 있는 경우에만 정보주체가 아닌 사용자에게 제공할 수 있음

4. 결론 및 시사점

▶ 데이터법은 데이터 거버넌스법, EU 보건 데이터 공간(European Health Data Space) 프로젝트, EU 공동 데이터 공간(Common European Data Spaces) 등과 더불어 EU의 데이터 접근성을 개선하고 시장 경쟁력을 촉진할 수 있는 잠재력을 보유

- 동법이 클라우드 제공업체에 제시하는 새로운 계약 의무와 데이터 서비스·클라우드 상호운용성을 위한 표준을 제시함에 따라, 사용자들은 비용 부담 없이 데이터와 애플리케이션을 한 제공업체에서 다른 제공업체로 쉽게 옮길 수 있을 것으로 예상

- EU는 데이터법의 시행을 통해 '28년까지 EU 회원국이 약 2,700억 유로의 GDPR 가치를 추가 창출할 수 있을 것으로 전망

▶ 데이터법은 사용자에게 스마트 가전제품 및 지능형 산업 기기 등의 사용으로 생성된 데이터에 액세스할 수 있는 권한을 제공하며, 이는 그동안 제품 제조자와 관련 서비스 제공자가 독점적으로 수집해왔던 데이터임

▶ 데이터에 대한 통제력이 강화되고 데이터를 공유할 수 있는 방법이 다양해지면서 기업들은 제품 및 관련 서비스의 데이터 중심적인 측면을 기반으로 혁신이 가능

- 제품 또는 관련 서비스를 제공하는 기업은 데이터에 대한 사용자 접근 및 제3자와의 데이터 공유 증가가 가져올 영향을 파악하고, 데이터 흐름을 촉진하는 프로세스를 구현하는 데 집중할 필요가 있음

- 특히 데이터법의 적용 범위가 포괄적이고 광범위한 의무를 수반하는 만큼, 기업들은 데이터 처리 및 제품 설계 전략을 전면적으로 재검토하여 관행을 조정해야 함

▶ 다만, 데이터법이 규정 위반에 대한 과징금 산정 기준 등 행정처분과 관련한 구체적인 사항은 각 국가에서 정하도록 위임하고 있기에, EU전역에 걸친 일관적인 집행은 보장하기 어려울 것으로 보임

Reference

1. European Commisison, A European Strategy for data, 2024.1.12.
2. European Commission, Data Act – Factsheet, 2022.2.14.
3. European Commission, European Data Act enters into force, putting in place new rules for a fair and innovative data economy, 2024.1.11.
4. European Commission, Data Act enters into force: what it means for you, 2024.1.11.
5. Hogan Lovells, Deep Dive on the new EU Data Act, 2023.12.7.
6. JDSUPRA, The European Data Act: New Rules for a New Age, 2023.12.26.
7. Pinsent Masons, EU Data Act entering into force 'should spur business action', 2024.1.11.
8. White&Case, The Data Act – the EU's bid to "ensure fairness in the digital environment and a competitive data market" – has been adopted, 2023.11.30.

EU 내 메타의 무광고 유료 서비스 모델의 개인정보 침해 이슈 분석

[목 차]

1. 개요

2. 배경 및 경과

3. noyb의 민원 제기와 메타의 입장
(1) noyb의 민원 제기
(2) 메타의 입장

4. 유럽 내 주요 개인정보 감독기관 및 규제 기관의 대응
(1) 오스트리아 DPA, FAQ 게재 통해 메타에 경고
(2) 선임 감독기관 아일랜드 DPC, 메타의 GDPR 위반 여부 조사 착수
(3) EDPB, 유럽 차원의 대응 조치 개입 가능성
(4) 프랑스 CNIL, 쿠키 페이월에 대한 사례별 분석을 통한 판단 필요
(5) 덴마크 DPA, 쿠키 페이월 적용 시 동의 자발성 강조
(6) 독일, '개별적 동의'로 국내 개인정보 감독기관 합의 도출

5. 평가 및 시사점

1. 개요

▶ 프라이버시 권익 단체인 noyb*는 메타(Meta)의 구독제 기반 '무광고 유료 서비스(subscription for no ads)'가 EU의 GDPR을 위반하고 있다며 오스트리아 개인정보 감독기관(DPA, Austrian Data Protection Authority)에 민원을 접수('24.1.)

* noyb(none of your business)는 오스트리아의 변호사이자 활동가인 막스 슈렘스(Max Schrems)가 대표로 있는 단체. 막스 슈렘스는 '20년 EU사법재판소(CJEU, Court of Justice of the European Union)가 EU-미국 간 개인정보 이전의 근거가 된 프라이버시 실드(Privacy Shield)를 무효화(슈렘스 판결)시키는 등 개인정보보호 분야의 주요 판결을 끌어내는데 주도적인 역할을 담당

- 앞서 '23년 11월, noyb는 메타가 사용자 추적을 중단하기 위해 부과하는 비용이 사용자당 창출하는 가치에 비해 '지나치게 비례성을 벗어난다(way out of proportion)'라고 지적하며 과도한 요금제 적용의 문제점을 오스트리아 DPA에 제기한 바 있음

- 아울러 noyb는 이와 별도로 '24년 1월, 메타는 사용자가 추적 동의를 철회하는 절차를 지나치게 까다롭게 설계했다는 점을 문제점으로 제기하며 GDPR 위법성을 다시금 지적

▶ 현재 오스트리아 DPA는 본 건을 CJEU에 회부하기에 앞서, 동 기관 웹사이트의 FAQ 페이지를 통해 메타의 시장 내 준독점적 지위로 인한 '서비스 유료화'가 '동의' 방식*을 대신하기 어렵다는 취지의 게시물을 공개

* ▲지불 또는 동의(pay or consent) ▲쿠키 월(cookie walls) ▲쿠키 페이월(cookie paywalls) 등으로 표현. 사용자가 쿠키 사용에 동의하면 웹사이트에 무료로 액세스할 수 있는 메커니즘으로, 사용자가 동의하지 않을 때는 요금 결제 후 웹사이트에 액세스할 수 있음.

- 이외에도 타 EU 회원국 개인정보 감독기관들이 메타의 무광고 유료 서비스에 대해 GDPR 위반 의혹을 제기하고 있는 상황

2. 배경 및 경과

▶ EU는 앞서 '22년 12월과 '23년 7월, 메타가 맞춤형 광고 목적으로 EU 내 정보주체의 행태정보를 수집하는 행위에 대한 법적 근거를 무효화시킨 바 있음

- '22년 12월, 아일랜드 개인정보 감독기관(DPC, Data Protection Commission)은 메타 아일랜드에 ▲페이스북 서비스 관련 GDPR 위반으로 2억 1,000만 유로 ▲인스타그램 서비스 관련 위반으로 1억 8,000만 유로의 과징금을 각각 부과

- 이러한 조치는 메타의 행태정보 기반 맞춤형 광고*를 위한 개인정보 처리의 근거가 GDPR에서 규정하는 계약상의 필요성에 의한 것이 아니라는 EU개인정보보호이사회(EDPB, European Data Protection Board)의 구속력 있는 결정에 따른 것

* 사용자의 온라인 행동에 대한 정보를 활용하여 더욱 관련성이 높고 맞춤화된 광고를 제공하는 온라인 광고의 한 형태

- 또한 이러한 개인 맞춤형 광고를 위해 정보주체의 사전 동의를 취득할 것을 의무화함으로써 EU 내 메타의 광고 모델에 직접적인 변화를 초래

▶ '23년 7월, CJEU는 독일의 반독점 감시 기관인 연방카르텔청(FCO, The Federal Cartel Office)이 메타에 대해 사용자 동의 없이 소셜 플랫폼 전반에서 사용자 개인정보를 결합하는 이른바 슈퍼프로파일링(superprofiling) 행위를 중단해야 한다는 명령에 대한 메타의 이의 제기와 관련하여, FCO의 판단을 인정하는 판결을 내림[6]

▶ 이후 '23년 10월, 메타는 무광고 유료 서비스 제공과 함께 동의 기반 추적 방식으로 전환할 것을 발표

- 이에 페이스북과 인스타그램에서 행태정보 추적 및 프로파일링을 원하지 않는 사용자는 광고 없는 버전의 서비스에 액세스하기 위해 월간 구독료를 지불해야 함
- 한편, 서비스를 계속 무료로 이용하고자 하는 페이스북 및 인스타그램 사용자는 추적에 '동의'해야 하며, 메타는 이러한 동의 행위가 GDPR에 따라 합법적이라고 주장

▶ 그러나 noyb는 동의 대체 수단으로서 무광고 유료 서비스의 과금수준에 대한 적정성과 동의 철회의 어려움을 들어 GDPR 위반 문제를 제기

표 _ 메타의 맞춤형 광고 관행 관련 EU 내 개인정보보호 조치 경과

시점	주체	조치 내용
2022.5	프랑스 CNIL	▪ 쿠키 페이월(cookie paywalls)의 합법적 사용 평가 기준을 발표 ▪ 쿠키 페이월을 전면 금지하는 것은 경우에 따라 동의의 자유를 해칠 수 있다는 점을 지적하며, 사례별로 동 기준을 적용해야 함을 강조
2022.12	EU개인정보보호 이사회(EDPB)	▪ 행태정보 기반 광고 제공을 위해 메타가 수행하는 개인정보 처리가 적합한 법적 근거에 기반하지 않았다고 결론 ▪ 이에 따라 메타에 개인정보 처리 규정을 준수하고 불법적인 처리를 중단할 것을 요청
2022.12.	아일랜드 DPC	▪ 행태정보 기반 광고 목적의 개인정보 처리에 대한 위법 판결에 따라 페이스북에 2억 1,000만 유로, Instagram에 1억 8,000만 유로의 과징금을 각각 부과
2023.3	독일 연방 및 각 주(州) 개인정보 감독기관 컨퍼런스(DSK)	▪ 메타가 제공하는 서비스의 GDPR 요건을 충족하기 위한 포괄적 동의의 필요성 합의
2023.7	CJEU, 독일 FCO	▪ 사용자 동의 없이 소셜 플랫폼 전반에서 사용자 정보를 결합하는 슈퍼프로파일링(superprofiling) 행위 중단 명령
2023.10	메타	▪ 무광고 유료 서비스 모델 도입을 통해 동의 기반 추적 방식 전환 발표
2023.11	noyb(1차)	▪ 메타의 동의 철회의 일환으로 적용되는 무광고 유료 서비스의 과도한 조치에 대해 오스트리아 DPA에 문제를 제기
2023.12	오스트리아 DPA	▪ 동의 철회에 대한 과금 관련 방침을 FAQ로 게재
2024.1	noyb(2차)	▪ noyb가 메타의 사용자 추적 동의 철회 절차가 지나치게 까다롭다고 오스트리아 DPA에 문제를 제기

출처: 넥스텔리전스(주)

6) TechCrunch, CJEU ruling on Meta referral could close the chapter on surveillance capitalism, 2024.7.4.

3. noyb의 민원 제기와 메타의 입장

(1) noyb의 민원 제기

▶ '23년 11월 오스트리아 DPA에 접수한 noyb의 첫 번째 이의 제기는 메타가 사용자를 추적하지 않기 위해 부과하는 비용*이 사용자당 창출하는 가치에 비해 '지나치게 과도하다'라는 주장에 초점을 맞추고 있음

* 연결 계정당 웹에서는 월 9.99유로, 모바일에서는 월 12.99유로

▶ '24년 1월의 두 번째 이의 제기에서는 메타가 이용자 서비스 계약에 따라 사용자가 추적 동의를 철회하는 절차를 지나치게 까다롭게 했다는 점을 지적[7)]

- 즉, 메타가 마련한 절차상에서 동의를 철회하려면 사용자는 광고 없는 월간 구독 서비스에 가입해야 하지만 추적에 대한 동의는 단 한 번의 '확인' 클릭 동작만으로 매우 간단하게 이뤄진다는 것

- GDPR*에 따르면 사용자는 동의를 쉽게 철회할 수 있어야 하나, noyb는 메타의 사용자가 자신의 개인정보 보호를 위한 동의 철회를 위해 비용을 지불해야 한다는 점을 지적

  * GDPR 제7조는 '동의의 철회는 동의의 제공만큼 용이해야 한다'라고 명시하고 있지만, 원클릭으로 이뤄진 동의를 '철회'하기 위해서는 251.88유로의 구독료를 지불하는 방법 이외에는 없다는 것

- noyb는 오스트리아 DPA가 메타에게 GDPR을 준수하여 처리 작업을 수행하고 사용자에게 수수료 없이 쉽게 동의를 철회하는 방법을 제공하도록 명령해야 한다고 주장하며, 추가적인 GDPR 위반 가능성을 방지하기 위해 벌금 부과를 촉구

- 또한, noyb는 오스트리아 DPA에 대해 긴급 절차(urgency procedure)*를 발동할 것을 요청

  * GDPR 66조에서 규정된 긴급 절차는 개인정보 권리에 대한 잠재적 위반 가능성이 있는 문제에 대해 즉시 해결하기 위해 감독기관이 취할 수 있는 개인정보 보호 조치. 개인정보 침해가 고위험, 임박한 피해 또는 공익 저해를 초래하는 경우 등이 조치를 취할 수 있는 사안에 해당

- noyb는 긴급 절차 발동 여부 결정과 관련된 DPA의 재량권이 장기간 개인정보 보유에 '개인정보 보호 권리를 효과적으로 보호해야 할 의무'에 의해 제한된다는 최근 CJEU 판례[8)]*를 인용하며, 메타의 경우에서도 개인정보 주체가 긴급 절차를 요청할 권리가 있다고 주장

  * CJEU는 Schufa라는 독일 신용정보 기관은 공공 파산등록부(German public insolvency register)가 6개월 이상의 장기간 데이터 보유를 제한한다고 판시. 개인이 경제 생활을 재개하기 위해서는 잔여 채무 면책이 중요하나 Schufa의 개인정보 보유 관행은 개인의 신용 점수에 중대한 영향을 미칠 수 있으므로 이를 제한했다는 점에서 정보주체의 권리와 이익을 보호하기 위해 조치의 효율성과 신속성을 강조한 판례

7) TechCrunch, Meta's EU ad-free subscription faces early privacy challenge, 2023.11.28
8) TechCrunch, Credit scoring firms face curbs after landmark EU data protection ruling, 2023.12.7

(2) 메타의 입장

▶ 메타의 매튜 폴라드(Matthew Pollard) 대변인은 noyb의 이의 제기에 대한 공식 성명은 자제해 오고 있으며, '23년 7월 CJEU의 개인정보 처리를 위한 동의 획득 대안으로 광고 없는 구독제 유료 서비스 모델을 승인했다는 점을 강조

- 메타는 '23년 10월 EU에서 페이스북과 인스타그램 사용자를 위한 무광고 유료 서비스 제공의 법적 근거를 설명한 블로그 게시물[9]을 언급하며, 최근 몇 년간 주요 EU 규제 기관들과 법원이 공유한 최신 규제, 지침 및 판결을 대처하고 있다는 점을 설명

- 또한 폴라드 대변인은 메타가 사용자에게 제공한 선택권, 즉 ▲행태정보 추적을 허용하고 서비스에 자유롭게 액세스하거나 ▲광고 없는 액세스를 위해 메타에 일정 비용을 지불하는 것은 'EU 최고 법원의 지침에 부합한다*'고 강조

  * 앞서 CJEU는 '23년 7월, 사용자가 맞춤형 광고를 위한 개인정보 처리에 동의하는 방법의 대안으로 구독제 유료 서비스 모델을 인정한 바 있음

- 이 외에도 프랑스, 덴마크, 독일 등 다수 EU 개인정보 감독기관에서 동의 취득 수단으로서 구독 서비스의 유효성을 인정한 바 있음을 주장

4. 유럽 내 주요 개인정보 감독기관 및 규제기관의 대응

(1) 오스트리아 DPA, FAQ 게재 통해 메타에 경고

▶ '23년 12월, 오스트리아 DPA는 쿠키와 개인정보보호를 주제로 게재한 공식 홈페이지 FAQ 섹션에서 맞춤형 광고 동의와 관련해 논란이 된 '지불 또는 동의(pay or okay)' 이슈에 관해 언급

- 해당 FAQ에서 오스트리아 DPA는 웹사이트 접속에 대한 비용을 지불하는 것이 '동의를 대신할 수 있는 대안이 될 수 있다'는 입장을 표명

- 그러나 ▲동의가 구체성을 띄고 ▲해당 기업이 시장에서 '독점' 또는 '준독점' 지위를 갖고 있지 않으며 ▲대안으로 지불하는 비용이 '적절하고 공정'하며 '터무니없이 비현실적으로 높은 가격으로 제공'되지 않는 등 GDPR을 완벽히 준수하는 경우에 한한다고 명시

- 한편, 오스트리아 DPA는 '지불 또는 동의'에 대한 CJEU의 판례가 아직 없는 점을 지적하며, 동 FAQ의 내용이 현재까지의 DPA 입장임을 강조

  ※ 현재 다수의 개인정보 보호 전문가들은 이 문제가 결국 CJEU에 회부될 것으로 예상

9) 메타, Facebook and Instagram to Offer Subscription for No Ads in Europe, 2013.10.30

(2) 선임 감독기관 아일랜드 DPC, 메타의 GDPR 위반 여부 조사 착수

▶ 일반적으로 메타를 상대로 EU 회원국 DPA에 제기되는 민원은 GDPR의 원스톱숍(OSS, One-Stop-Shop)* 메커니즘에 따라 메타의 선임(lead) 감독기관인 아일랜드 DPC에 다시 회부

* GDPR 제56조(선임 감독기관의 법적 자격)에 따르면, 컨트롤러가 복수의 EU 국가에서 활동하는 조직일 경우, 컨트롤러의 주 사업장(main establishment)이 위치한 국가의 개인정보 감독기관을 선임 감독기관으로 지정하여 여러 회원국과 관련된 조사를 조정할 책임을 부과함

▶ 아일랜드 DPC는 메타가 '23년 여름에 무광고 유료 서비스 출시 가능성을 최초 언급한 이래로 해당 서비스 모델에 대한 검토를 진행해 온 것으로 알려짐

- 다만, 아일랜드 DPC가 메타의 동의 방식에 대한 검토를 정식 조사 단계로 전환하더라도 동 사안에 대한 최종 결정을 내리기까지 조사가 수년 동안 진행될 것으로 예상
- 또한, DPC의 최종 결정 역시 사실상 EU 개인정보 감독기관 간의 의견 차이 조율을 담당하는 EDPB의 지시에 따른 것이므로, 개인정보 감독기관들이 직접 문제를 해결하기로 결정하지 않는 한, 메타의 동의 조작에 대한 신속한 개인정보 보호 단속은 어려울 것으로 전망

(3) EDPB, 유럽 차원의 대응 조치 개입 가능성

▶ GDPR은 국경 간 처리와 관련된 불만사항을 처리하기 위한 원스톱 숍(OSS) 규정을 통해 현지 DPA가 현지 사용자를 보호할 수 있도록 자국 시장에서 개인정보 침해 위험을 완화하기 위한 조치를 취할 수 있도록 EDPB에 긴급 권한(emergency power) 발동 요청이 가능

- 실제로 '23년 11월 노르웨이 DPA는 메타의 광고에 대해 적법성 결여를 주장하며 행동 광고를 목적으로 한 개인정보 처리 금지 규정을 노르웨이 현지에서와 같이 유럽 전역으로 확대하여 적용할 것을 EDPB에 요청

▶ EDPB는 이를 수용하여 긴급 강제 결정(urgent binding decision)으로 노르웨이 현지와 동일한 조치를 유럽경제지역(EEA) 전체에 걸쳐 적용할 것을 발표[10)]

- EDPB의 아누 탈루스(Anu Talus) 의장에 따르면 'EDPB는 이미 2022년 12월, 행동 광고를 위해 메타가 수행하는 개인정보 처리가 적합한 법적 근거에 기반 하지 않는다는 점을 명확히 한 바 있다'라며, '메타는 개인정보 처리 규정을 준수하고 불법적인 처리를 중단해야 한다'라고 언급

10) EDPB, EDPB Urgent Binding Decision on processing of personal data for behavioural advertising by 메타, 2023.11.1

- 하지만 그 당시 이미 메타는 동의 기반 추적 방식으로 전환한 상태로, 규제 당국의 개입을 피할 수 있었던 상황

- 이 사례는 법 집행이 지연되는 과정에서 법률 위반 기업은 집행 자체를 회피할 수 있다는 사실을 시사

(4) 프랑스 CNIL, 쿠키 페이월에 대한 사례별 분석을 통한 판단 필요

▶ 프랑스 개인정보 감독기관 CNIL의 지침[11]은 메타의 블로그 게시물을 직접적으로 언급하며 소위 '쿠키 페이월(cookie paywalls)'에 대한 '사례별' 분석이 필요하다는 점을 강조하며 다음의 사항을 언급

- 특정한 정보 추적 주체와의 거래 하에 서비스 제공 또는 웹사이트 접속을 하는 것은 경우에 따라 동의의 자유를 해칠 수 있음

  - 사용자가 모든 추적을 거부하고자 하는 경우 서비스 제공사가 '사이트에 대한 액세스를 허용하고 개인정보 사용에 동의하지 않아도 되는 실질적이고 공정한 대안(a real and fair alternative)'을 제공할 것을 권고

- 지배적 또는 필수 서비스 제공자와 같은 독점 서비스의 경우 인터넷 사용자의 선택권은 해당 서비스가 제공된 사이트에서만 가능하기 때문에 제약이 발생할 수 있음

  - 이 경우 정부 추적 주체의 접근 동의를 요구하는 서비스 제공자는 인터넷 사용자의 실질적인 선택권을 박탈할 수 있는 불균형이 존재할 수 있다는 점에 특히 주의해야 해야 하므로, 해당 제공자는 사용자가 대안적 서비스에 대해 용이한 접근성을 보장해야 함

- 서비스 제공사가 콘텐츠 액세스에 대해 부과하는 모든 요금은 합리적이어야 하며, 인터넷 사용자에게 더 큰 투명성을 보장하기 위해 부과된 요금에 대한 정당성에 대해 상세히 밝힐 것을 권장

  - 맞춤형 광고와 편집 콘텐츠의 개인화는 서로 상이한 목적의 서비스로, 서비스 액세스에 적용되는 목적을 결정할 때 구분이 되어야 한다고 명시함으로써, 부당하게 동의를 번들링화 하려는 서비스 제공자의 시도에 대해 경고

  - 메타의 경우 사용자는 추적에 동의하거나 비용을 지불하고 콘텐츠에 '광고없이' 액세스 하는 것 중 하나만 선택하도록 하고 있다고 지적

11) CNIL, Cookie walls: the CNIL publishes the first evaluation criteria, 2022.5.16.

(5) 덴마크 DPA, 쿠키 페이월 적용 시 동의 자발성 강조

▶ 덴마크 DPA(The Danish Data Protection Agency)의 쿠키월 지침[12]에 따르면, 서비스 제공사가 쿠키 페이월을 적용할 때 동의의 자발성을 강조하며 다음과 같이 적시

- 위법성 판단의 여부는 방문자가 동의 대신 콘텐츠 또는 서비스에 대한 액세스 비용을 지불할 수 있는 접근 방식이 자발적 요건을 충족하는지, 그리고 이 경우 이 접근 방식이 어떤 요건을 충족해야 하는지에 달려있음
- 또한 '지불 또는 동의'의 적법성에 대해 '일반적으로 명확성이 부족하다'고 명시
- 그러나 적법성 여부를 평가하기 위한 기준의 하나로, 결제 대안에 대한 '합리적인 가격' 설정을 들고 있는데, 덴마크 DPA는 '대안의 가격이 너무 높아서 방문자의 선택의 자유가 현실적으로 불가능하게 되어서는 안 된다'는 점을 강조

▶ 개인정보 처리에 대한 동의의 유효성을 평가할 때는 무엇보다도 사이트 방문자에게 만족스러운 대안이 제공되었는지를 우선적으로 고려해야 함

- 이를 위한 DPA의 평가 기준으로는 ▲합리적인 대안(서비스 유료화 등) ▲합리적인 가격(쿠키 월 적용 시) ▲목적에 부합한 동의 요청 여부(개인정보 수집 최소화 등) 등을 꼽고 있음

(6) 독일, '개별적 동의'로 국내 개인정보 감독기관 합의 도출

▶ 독일은 '23년 3월 독일 연방 및 각 주(州) 개인정보 감독기관 컨퍼런스(DSK)의 결정[13]을 통해 동의의 '자유로운 제공(freely-given)'을 포함하여 모든 GDPR 요건을 충족하기 위한 동의의 필요성을 강조

- 개인정보 감독기관들은 또한 '원칙적으로' '지불 또는 동의'가 가능하다고 명시하고 있으나 이 결정은 또한 다양한 처리 목적에 대해 포괄적으로 '모두 동의'하는 것에 대해 주의할 것을 경고
- 특히 '서로 크게 다른 여러 처리 목적이 있는 경우 세분화된 기준으로 동의를 받을 수 있는 방식으로 자발성 요건을 충족해야 한다'고 적시
  - 무엇보다도 사용자는 각각의 목적에 따라 동의 여부를 선택할 수 있어야 하며, 이러한 목적은 사용자가 적극적으로 선택할 수 있어야 함(옵트인)

12) https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/cookies/cookie-walls
13) DSK, Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 22., 2023.3

- 목적이 매우 밀접하게 관련된 경우에만 목적들의 번들링을 고려할 수 있기 때문에 이러한 측면에서 서로 다른 목적에 대한 포괄적인 전체 동의는 허용되지 않음

5. 평가 및 시사점

▶ EU 내에서는 CJEU의 승인 하에 동의를 대신할 수 있는 대안으로 무광고 유료 서비스(Pay or Okay) 모델의 등장이 디지털 마케팅 구조의 변화를 초래할 수 있을 것으로 주목 받아왔음

▶ 그러나 메타의 새로운 비즈니스 모델에 대한 EU 규제기관들의 입장 표명을 통해 나타난 바와 같이, EU 주요국의 규제 당국들은 광고 없는 유료 모델 도입 시 이용자 입장에서 선택의 구체성, 적절한 가격대 설정, 복잡한 동의 철회 절차 및 서비스 제공사의 시장 지위 등 사용자에게 미치는 다양한 영향이 동시에 고려되어야 적법성을 담보할 수 있다는 것으로 논의의 가닥이 잡히고 있는 상황

▶ 나아가 페이스북과 인스타그램의 경우 지배적 서비스 제공사인 동시에 메타의 네트워크 효과로 인해 소셜 네트워킹 공간에서 지속적인 영향력을 행사하고 있는 점을 고려하면 필수 서비스에도 해당될 가능성이 큼

▶ 따라서 CNIL을 비롯한 유럽 내 주요국 개인정보 감독기관들은 메타에 대해 동사 제공 서비스의 비추적(non-tracking) 버전에 대한 접근 용이성 확보 요구와 함께 규제 압박을 강화할 것으로 예상

- 실제 noyb가 주장하고 있는 바와 같이 사용자에게 신용카드를 발급하고 지속적인 수수료를 지불하도록 요구하는 것은 '접근의 용이성'으로 보기 어렵다는 것이 대부분 규제 당국의 이해

- 또한, 오스트리아 DPA 지침 등에서는 메타의 소셜 네트워크처럼 '시장에서 독점 또는 준독점적 지위를 가진 기업'의 경우 페이월이 적절하지 않은 점 역시 메타의 무광고 유료 서비스 관련 법리 대응에 불리한 요소로 작용할 것으로 관측

Reference

1. DSK, Beschluss der Konferenz der unabhangigen Datenschutzaufsichtsbehorden des Bundes und der Lander vom 22., 2023.3
2. EDPB, EDPB Urgent Binding Decision on processing of personal data for behavioural advertising by Meta, 2023.11.1
3. TechCrunch, CJEU ruling on Meta referral could close the chapter on surveillance capitalism, 2024.7.4.
4. TechCrunch, Credit scoring firms face curbs after landmark EU data protection ruling, 2023.12.7.
5. TechCrunch, Meta faces another EU privacy challenge over 'pay for privacy' consent choice, 2024.1.11.
6. TechCrunch, Meta's EU ad-free subscription faces early privacy challenge, 2023.11.28

<2024년 개인정보보호 월간 동향 보고서 발간 목록>

번호	호수	제 목
1	1월 01	EU 데이터법(Data Act) 주요 내용 분석 및 시사점
2	1월 02	EU 내 메타의 무광고 유로 서비스 모델의 개인정보 침해 이슈 분석

2024

개인정보보호 월간동향분석 제1호

발 행 2024년 2월 20일

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