

# PRiVACY REPORT

## 개인정보보호 월간동향분석

2024년 8월호



| CONTENTS |

2024년 8월호

1

EU GDPR과 LLM 간 관계성 분석

2

구글, 크롬 서드파티 쿠키 지원 종료 계획 철회  
- 최신 동향 분석 및 관련 기관 대응 중심으로 -

# EU GDPR과 LLM 간 관계성 분석



## [목 차]

### 1. 개요

### 2. 함부르크 개인정보 감독기관(HmbBfDI) 백서 주요 내용

- (1) AI 시스템과 LLM의 구별
- (2) LLM 관련 기술적 검토
- (3) LLM의 개인정보 저장
- (4) 실무적 시사점

### 3. 결론

#### 1. 개요

■ 8월 초부터 발효되는 EU AI법을 앞두고 독일의 함부르크 개인정보 감독기관(HmbBfDI)이 일반 개인정보보호 규정(GDPR)과 대규모 언어모델(LLM)\*의 관계를 다룬 백서를 발표('24.7.15.)

\* Large Language Model(LLM)은 인터넷에서 수집한 방대한 텍스트 데이터 학습을 기반으로 하여 인간의 언어를 이해하고 생성할 수 있는 인공지능 모델(예: 챗GPT) 혹은 기술을 의미함. 입력된 텍스트의 맥락을 이해하고 문장을 생성하는 등 다양한 언어 작업을 수행하며, 특정 목적에 맞게 추가 훈련이 가능함.

- 독일 함부르크 개인정보 감독기관(Hamburg Commissioner for Data Protection and Freedom of Information, 이하 HmbBfDI)은 대규모 언어모델(Large Language Model, 이하 LLM) 기술과 관련된 개인정보보호 문제를 다루는 기업과 당국을 지원하고, 추후 논의를 촉진하는 것을 목적으로 해당 백서<sup>1)</sup>를 발표
- 동 백서는 LLM의 기술적 측면을 설명하고, GDPR에 관한 EU 사법재판소(Court of Justice of the European Union, 이하 CJEU)의 관련 판례에 비추어 LLM과 GDPR 간 관계를 평가하며, 이에 따른 실무적 시사점을 제시

■ LLM의 출력 시 개인정보가 포함될 수 있다는 우려에 대해 개인정보가 LLM에 저장되는지 여부에 초점을 맞추고 있으며, LLM의 GDPR 적용과 관련하여 세 가지 명제 도출

1) HmbBfDI, Discussion Paper: Large Language Models and Personal Data, 2024.7.15.

- 첫 번째 LLM이 단순히 저장하는 것은 GDPR이 제4조제(2)항에서 규정한 개인정보의 ‘처리(processing)’에 해당하지 않음
  - 다만, LLM 기반 AI 시스템에서 개인정보가 처리되는 경우에는 GDPR 요건을 준수해야 함
- 두 번째 LLM에는 개인정보가 저장되지 않으므로, GDPR에 정의된 정보주체의 권리가 모델 자체와 관련이 없음
  - 그러나 접근, 삭제, 정정 요구 등의 정보주체 권리는 책임 있는 제공자나 배포자의 AI 시스템 입력 및 출력과 관련하여 행사 가능
- 세 번째 개인정보를 사용한 LLM 훈련은 관련 개인정보보호 규정을 준수해야 함
  - 이 과정에서 정보 주체의 권리 또한 지켜져야 하나, 훈련 단계에서의 잠재적 위반이 AI 시스템 내 해당 모델 사용의 적법성에는 영향을 미치지 않음

## 2. 함부르크 개인정보 감독기관(HmbBfDI) 백서 주요 내용

### (1) AI 시스템과 LLM의 구별

#### ■ AI 시스템은 여러 구성 요소로 이루어져 있고, LLM은 이러한 구성 요소 중 하나로 볼 수 있음

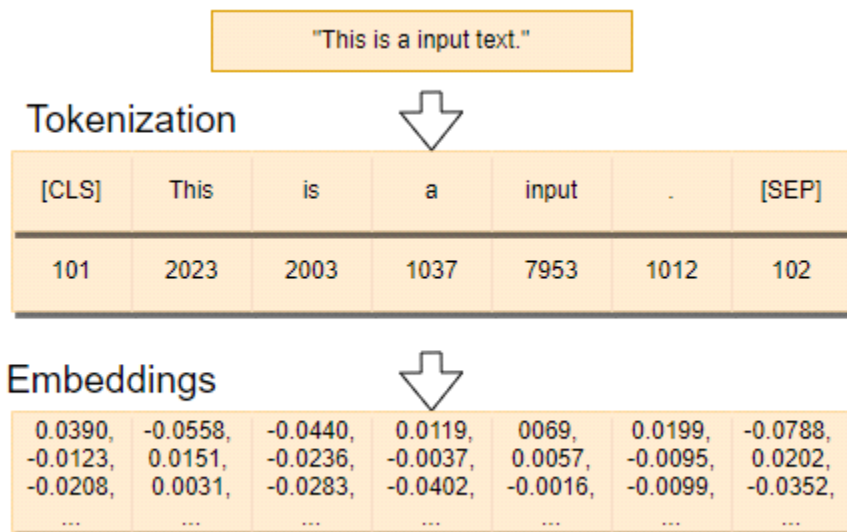
- LLM이 AI 시스템의 구성 요소로서 프롬프트(prompt)를 처리\*할 때, 특히 프롬프트에서 구체적인 요청이 있는 경우 LLM이 자연인과 관련된 정보를 출력할 수 있다는 점에서 개인정보가 LLM에 저장되는지에 대한 의문이 제기
  - \* 이같이 결론을 도출하는 과정은 ‘추론(inference)’이라고도 함
- 이러한 의문을 해결하기 위해서는 LLM의 기술적인 측면을 검토하기 이전에 AI 시스템과 AI 시스템에 통합될 수 있는 LLM을 구분하는 것이 중요
- AI 시스템은 여러 구성 요소(사용자 인터페이스, 입력 및 출력 필터, LLM 등)로 이루어져 있고, 이러한 구성 요소 없이는 시스템을 의미 있게 사용할 수 없음
  - 사용자 입력은 일반적으로 LLM이 추론되기 전에 AI 시스템의 다른 구성 요소에 의해 먼저 처리\*되며, 이후 LLM에서 생성된 원시 출력은 일반적으로 인터페이스를 통해 사용자에게 표시되기 전에 필터에 의해 추가 처리되는 과정을 거침
  - \* 예를 들어, 사용자 입력(프롬프트)은 데이터베이스, 인터넷 검색 등을 통해 추가 정보로 보강될 수 있고, 이후 LLM이 수정된 프롬프트를 처리
- 동 백서에서는 개인정보가 LLM에 저장되는지에만 초점을 맞추고, 전체 AI 시스템의 처리 활동을 평가하지는 않음

## (2) LLM 관련 기술적 검토

### I (정보 처리의 기본 요소, 토큰) 언어 정보가 LLM에서 처리되기 위해서는 모든 입력 텍스트가 미리 정의된 비교적 작은 덩어리인 '토큰(token)'으로 나뉘는 '토큰화(tokenization)'가 수행됨

- LLM은 일반적으로 여러 언어를 처리하고, 처음에는 관련 언어로 된 대량의 텍스트 입력으로 학습되며, 그다음에는 언어적 결과를 출력으로 제공하게 됨
- 모든 텍스트는 LLM에 들어가기 전에 미리 정의된 비교적 작은 덩어리인 '토큰(token)'으로 나뉘며, 이러한 조각은 일반적으로 전체 단어보다는 작지만 개별 글자보다는 큼
- 텍스트 조각인 토큰은 이후 모델 내에서만 사용되는 숫자 값으로 변환되므로, LLM 내에서 텍스트는 원래의 형태가 아닌 숫자 토큰 형태로만 저장
- 이러한 숫자 토큰은 단순한 인덱스일 뿐 토큰의 의미를 직접적으로 나타내는 것은 아니므로 '임베딩(embedding)'이라는 과정을 거쳐 추가적으로 처리
  - 임베딩은 토큰을 서로 연관 지어 배치함으로써(즉, 확률 가중치에 따라 토큰을 할당함으로써) 학습된 상관관계를 포착

**그림 1** 토큰화 및 임베딩 프로세스



출처 : Vaclav Kosar(2022.9.16.)

### I (정보 저장) 개별 토큰은 LLM 모델 내에 저장되지 않으며, 모델의 훈련 데이터에 개인정보가 포함되더라도 추상적인 표현으로 변환되는 과정을 통해 특정 개인의 구체적인 특징은 손실됨

- 개별 토큰은 언어적 조각일 뿐이며, 텍스트 또는 토큰은 모델 내 어디에도 저장되지 않음
- 일반적으로 최신 LLM에서 토큰 간 관계를 정의하는 파라미터는 수십억 개에 달하므로 전체 모델의 기능을 손상시키지 않고는 파라미터를 구체적으로 조정할 수 없음
- LLM의 학습 데이터에 개인정보가 포함되더라도 머신러닝 과정에서 추상적인 수학적 표현으로 변환하는 과정을 거치면서 특정 개인에 대한 구체적인 특징이 손실됨
  - 대신 모델은 학습 데이터 전체에서 도출된 일반적인 패턴과 상관관계를 포착
- 모델은 훈련에 사용된 텍스트를 원래 형태로 저장하지 않으며, 훈련 데이터 세트를 모델에서 완벽히 재구성할 수 없도록 처리
  - 다만 LLM은 문맥 관계에 따라 매우 구체적인 방식으로 훈련 텍스트를 처리하므로, 종종 유사한 출력 텍스트를 생성할 수 있다는 모순적인 특성을 가짐
- 그러나 LLM이 생성하는 모든 것은 이미 저장된 것을 단순히 재생산하는 것이 아니라 새로 생성되는 것으로, 이러한 확률적 생성 기능은 기존의 데이터 저장 및 데이터 검색과는 근본적으로 다름

### (3) LLM의 개인정보 저장

#### ■ 아직까지 LLM의 개인정보 저장에 대한 CJEU의 판결이 존재하지 않지만, HmbBfDI는 LLM이 GDPR 조항의 의미 내에서 개인정보를 저장하지 않는다고 결론지음

- 법적 용어로서의 '개인정보'(GDPR 제4조제1항<sup>2)</sup>)는 자연인과 '관련된' 식별되거나 식별 가능한 정보를 의미하며, 이는 일반 대중이 이해하고 있는 개인에 대한 정보 개념과는 상이함
  - 예를 들어, 도서관 카드에 일련의 숫자만 표시되어 있더라도 도서관 카드 번호와 관련된 개인이 도서관 데이터베이스와 같이 다른 수단을 통해 식별될 수 있는 경우, 해당 번호 자체를 개인정보로 간주할 수 있음
  - 단, CJEU는 개인정보의 개념을 고려할 때, '과도한 노력(disproportionate effort)'을 요구하지 않는 합법적인 식별 수단만을 감안해야 한다고 판시한 바 있음
    - ※ '16년 10월 19일 자 Breyer 판결(C-582/14)에서 CJEU는 개인 식별이 실질적으로 불가능한 경우에 대해 언급하며 disproportionate effort의 개념을 도입. 구체적으로 ▲법률에 따라 개인 식별이 금지된 경우, 또는 ▲개인을 식별하기 위해 시간, 비용, 인력 측면에서 과도한 노력이 필요한 경우, 개인 식별의 위험이 현실적으로 무시할 만한 수준인 것으로 간주.<sup>3)</sup>

2) GDPR 제1장(일반규정) 제4조(정의)제1항: 개인정보는 식별된 또는 식별 가능한 자연인('정보주체')과 관련한 일체의 정보를 가리킨다. 식별가능한 자연인은 직접 또는 간접적으로, 특히 이름, 식별번호, 위치정보, 온라인 식별자를 참조하거나 해당인의 신체적, 심리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성에 특이한 하나 이상의 요인을 참조함으로써 식별될 수 있는 자를 가리킨다.

3) CJEU, C-582/14, 2016.10.19. para. 46 참고. 해당 판례는 '유동IP'가 개인정보에 해당하는지 여부



- CJEU는 아직 LLM 또는 이와 유사한 기술의 개인정보 저장에 대한 판결을 내리지 않았지만, 이전 CJEU 판례와 알려진 LLM 공격 방법을 고려할 때, HmbBfDI는 LLM이 전문(Recital) 제26조<sup>4)</sup> 및 GDPR 제4조제1항 내지 제2항<sup>5)</sup>의 의미 내에서 개인정보를 저장하지 않는다고 결론

※ '23년 10월 발표된 덴마크 개인정보 감독기관(Danish Data Protection Authority)의 가이드라인<sup>6)</sup>에 따르면 AI 모델에는 어떠한 개인정보도 포함되지 않음. 단지 개인정보 처리의 결과로서 간주함. 이는 통계 보고서에 통계 분석의 결과인 결론과 집계된 데이터만 포함되어 있는 경우 개인정보로 간주되지 않는다는 사실에 따른 것임

- 개인정보 공격으로 훈련 데이터를 재생산하기 위해 미세 조정된(fine-tuned)\* LLM이 간혹 만들어지는 것이 관찰되었지만, 이러한 사례가 LLM에 개인정보가 저장된다는 법적 결론을 입증하는지는 의문시됨

\* 미세 조정은 특정 작업이나 사례에 맞게 사전 학습된 모델을 조정하는 것을 의미

## I (LLM에 포함된 토큰이 개인정보를 저장하는지 여부) CJEU에서 다루고 있는 개인정보 식별자(identifier)와는 달리, LLM에 저장된 정보에는 특정 개인과 연결되는 식별 정보가 포함되어 있음

- 앞서 CJEU는 개인정보와 관련하여 IP 주소, 시험 응답, 관공서의 법적 메모, 차량 식별 번호 또는 TC 문자열(TC string)\*과 같은 기타 코드화된 문자열 등을 고려함

\* Transparency and Consent String: 온라인 광고업계에서 사용되며, 광고 목적의 데이터 처리에 대한 사용자 동의와 선호도 등을 인코딩하고 이른 이해관계자들에게 전달하는 데 사용

- CJEU는 '개인정보'에 해당하는 대상은 식별자 또는 정보주체와 '관련된(related)\*' 정보이며, 여기서 '관련성(relevant)'은 식별자의 기능과 식별자에 포함된 정보에서 비롯된다고 판시<sup>7)</sup>

\* CJEU는 Nowak(C-434/16) 판례에서 정보가 개인과 '관련되어'있다는 것은 그 내용, 목적 또는 결과로 인해 특정 개인과 연결되어 있음을 의미한다고 해석<sup>8)</sup>

에 대해 독일 법원이 CJEU에 선결적 판결을 청구한 사례.

- 4) GDPR 전문26조: 개인정보 보호 원칙은 식별된 또는 식별될 수 있는 개인에 관한 일체의 정보에 적용된다. 가명처리를 거친 개인정보는 추가 정보의 사용으로 개인에 연계될 수 있는 정보로서, 식별 가능한 개인에 관한 정보로 간주되어야 한다. 개인이 식별 가능한지를 판단함에 있어 선별(singling out) 등 그 개인을 직간접적으로 식별하기 위해 컨트롤러 또는 제3자가 합리적으로 사용할 것으로 예상되는 모든 수단이 고려되어야 한다. 그 수단이 개인을 식별하는 데 사용될 것이라 합리적으로 예상되는지 여부를 확인하기 위해서 식별에 소요되는 비용 및 시간 등의 모든 객관적 요인을 고려하고, 처리 시점에 가용한 기술 및 기술 발전사항을 고려하여야 한다. 따라서 개인정보 보호 원칙은 익명정보, 즉 식별되었거나 식별 가능한 개인에 관련되지 않은 정보 또는 정보주체가 식별 가능하지 않거나 더 이상 식별 가능하지 않은 방식으로 익명 처리된 개인정보에는 적용되지 않는다. 따라서 본 규정은 통계 목적 또는 연구 목적 등을 위한 익명정보의 처리에는 적용되지 않는다.
- 5) GDPR 제1장(일반규정) 제4조(정의)제2항: 처리는 자동화 수단에 의한 것인지 여부에 관계없이 단일의 또는 일련의 개인정보에 행해지는 단일 작업이나 일련의 작업으로서, 수집, 기록, 편집(organisation), 구성, 저장, 가공 또는 변경(adaptation or alteration), 검색(retrieval), 참조(consultation), 사용, 이전을 통한 제공, 배포나 기타 방식으로의 제공(dissemination or otherwise making available), 연동이나 연계(alignment or combination), 제한, 삭제 또는 파기 등이 이에 해당한다.
- 6) Datatilsynet, Offentlige myndigheters brug af kunstig intelligens, 2023.10.
- 7) CJEU, C-434/16, 2017.12.20. para. 35; CJEU, C-487/21, 2023.5.4. para. 24; CJEU, C180/21, 2022.12.8. para. 70 참고

- (예시 1) IP 주소는 사용자가 온라인에서 데이터를 주고받을 수 있도록 장치를 할당하는데 사용되는데, 이는 온라인 활동과 실제 사람 사이의 관계적 연결(relational link)을 설정하기에 개인정보에 해당<sup>9)</sup>
- (예시 2) 차량 식별 번호는 제조사, 차종, 장비, 생산지, 제조 연도 등 차량 고유의 특성을 코드화하여 특정 차량을 식별하고, 간접적으로는 차량 소유자를 식별할 수 있게 하기에 개인정보에 해당<sup>10)</sup>
- 위와 같은 식별자는 특정 개인 또는 개인과 관련된 대상의 신원, 특성 또는 상황을 대신 나타내는 일명 ‘플레이스홀더(placeholder)’ 역할을 할 수 있음
- 그러나 CJEU 판례에서 다룬 상기 식별자 유형과는 달리, 개별 토큰은 개별 정보 콘텐츠가 부족하며 이러한 정보에 대한 플레이스홀더 기능이 없음
  - 토큰 간의 관계를 나타내는 임베딩조차도 학습된 입력의 수학적 표현일 뿐임
  - LLM은 개인과 ‘관련된’ 구체적인 특성 없이, 학습 데이터를 고도로 추상화하고 집계한 데이터 포인트와 그 관계만을 저장
  - LLM에 포함된 토큰에는 학습 데이터 세트 내 자연인에 대한 구체적인 정보가 포함되어 있지 않음
  - CJEU에서 정의하는 개인정보의 핵심 특징인 ‘개인과 직접적이고 표적화된 연관성(direct, targeted association to individuals)’이 LLM에 저장된 정보에는 결여되어 있음
  - 즉 CJEU의 기준에 따르면, LLM의 개인정보 저장 여부는 잠재적 컨트롤러가 사용할 수 있는 수단에 따라 달라지지 않음

**I (개인정보 공격 및 개인식별정보(PII) 추출의 영향) LLM이 개인정보를 포함한 데이터를 출력할 수 있다는 사실이 LLM이 개인정보를 저장(기억)하고 있다는 법적인 증거가 되기에는 부족하며, 이를 확인하기 위한 시도는 실질적으로 매우 어렵고 법적으로 금지되어 있을 가능성 존재**

- 미세 조정을 통해 특정 업무에 최적화된 LLM은 특정 상황에서 자연인과 관련된 정보를 포함한 학습 데이터를 재생산(reproduce)할 수 있다는 사실이 관찰된 바 있음
  - 이러한 사실로 미루어 자연인과 관련된 정보가 토큰이나 임베딩의 형태로 표현되더라도 LLM에 저장(‘기억’)되어 있을 것이라든 결론에 도달하게 됨
- 그러나 HmbBfDI는 이러한 유형의 추출이 개인정보가 LLM에 저장된다는 법적 결론으로 이어지는지에 대해서는 의문을 제기

8) CJEU, C-434/16, 2017.12.20. para. 34 참고. 해당 판례는 아일랜드 법원이 수습 회계사 Nowak이 제출한 서면 시험 답안의 개인정보 구성 여부에 대해 CJEU에 선결적 판결을 내려줄 것을 제정한 사례

9) CJEU, C-582/14, 2016.10.19. 참고

10) CJEU, C-319/22, 2023.11.9. 참고. 해당 판례는 차량 식별 번호(VIN)가 GDPR에서 정의하는 개인정보에 해당하는지에 관한 것



- 우선, LLM은 학습 데이터와 우연히 일치하는 텍스트를 생성할 수 있기 때문에 LLM 출력에 그럴듯한 개인정보가 있다는 것만으로 개인정보가 기억되었다는 결정적인 증거가 될 수는 없음
- 또한 개인정보의 재생산은 일반적으로 '개인정보 공격(privacy attacks)'이나 '개인식별정보(Personal Identifiable Information, PII) 추출(extraction)'과 같은 LLM에 대한 표적 공격을 통해서만 발생하나,
- CJEU 판례로 확립된 기준에 근거하여 정보를 개인정보로 분류하기 위해서는 ▲컨트롤러나 제3자를 통해 개인 식별이 가능해야 하며 ▲식별 방법이 법적으로 금지되지 않아야 하고 ▲식별에 과도한 시간, 비용, 인력이 소요되지 않아야 함
- 이에 LLM에 대한 공격 수행은 실질적으로 '과도한 노력'으로 간주될 수 있으며, 이러한 공격을 통한 개인정보 추출은 CJEU의 개인정보 분류 기준에 부합하지 않을 수 있음
- LLM에 대한 효과적인 개인정보 공격은 일반인의 능력을 크게 상회하는 전문 지식과 시간 투자를 요구
  - 현재 기술을 기반으로 LLM 생성 텍스트의 진위 확인을 위해서는 원본 학습 데이터에 대한 접근 권한이 필요하며, LLM 출력과 원본 데이터의 직접 비교만이 개인정보 저장 여부를 판단할 수 있는 근거로 성립
  - 그러나 LLM 학습 데이터 세트는 일반적으로 전체 공개되어 있지 않으며, 방대한 LLM 출력과 학습 데이터 간의 상관관계를 검증에는 막대한 양의 데이터가 필요함
- LLM 개발자들은 이러한 공격에 대비해 데이터 추출을 탐지하고 방지하기 위한 보호 조치를 지속해서 개선하는 중임
  - 기술적 보호 조치를 의도적으로 우회하는 행위는 독일 법률상 금지될 가능성이 있음

#### (4) 실무적 시사점

##### ■ LLM이 개인정보를 저장하지 않는다는 명제는 기업 또는 공공기관의 실무에서 중요한 의미를 지님

- (LLM의 불법적 학습 관련) 기업 또는 공공기관이 제3자가 개발한 LLM을 배포한 후 제3자가 법적 근거 없이 모델 학습에 개인정보를 사용했다는 사실이 밝혀지는 경우가 존재할 수 있음
  - 이와 같은 상황에서 모델 학습 중 잠재적으로 불법적인 개인정보 처리는 해당 모델 사용의 적법성에 영향을 미치지 않음
  - LLM 학습 과정에서 발생한 개인정보보호 위반에 대한 책임은 LLM을 배포한 관리자에게 귀속되는 것이 아니라 개발자에게만 있음

- LLM을 배포하고 미세 조정을 원하는 기업 및 당국과 마찬가지로 모델 개발자도 데이터 보호 규정을 준수해야 함
- (정보주체 권리 관련) 개인이 기업 또는 공공기관의 LLM 기반 챗봇에 자신의 이름을 입력했을 때, 해당 챗봇이 본인에 대한 잘못된 정보를 제공하는 경우가 발생할 수 있음
  - 조직은 개인정보를 처리할 때 GDPR을 준수해야 하지만, LLM은 개인정보를 저장하지 않으므로 GDPR 제12조<sup>11)</sup> 이하의 정보주체 권리 보장 의무의 적용 대상이 될 수 없음
  - 그러나 AI 시스템이 출력(output) 또는 데이터베이스 쿼리(query)를 통해 개인정보를 처리할 경우, 컨트롤러는 GDPR에서 규정한 정보주체 권리를 이행해야 함
  - 즉, 정보주체는 챗봇의 입력·출력값과 관련해 ① 접근권(GDPR 제15조) ② 정정권(GDPR 제16조) ③ 삭제권(GDPR 제17조) 등을 행사할 권리가 있음
- (LLM 미세 조정 관련) 기업 또는 공공기관이 제3자가 개발한 LLM을 특정 용도에 맞게 자체 훈련 데이터로 미세 조정하고자 하는 경우가 있을 수 있음
  - 이러한 경우, 기업 또는 공공기관은 학습 데이터에 개인정보를 최소한으로 포함해야 하며, 학습 목적에 적합한 경우 합성 데이터를(synthetic data)\* 우선순위로 두어야 함
    - \* 실제 데이터의 통계적 특성을 모방하여 인공적으로 생성된 데이터로, 개인정보보호와 데이터 가용성을 동시에 확보할 수 있는 방안.
  - 미세 조정에 개인정보를 사용할 경우, 반드시 법적 근거가 있어야 하며 정보주체의 권리를 보장할 방안을 마련해야 함
- (로컬 LLM 운영 관련) 기업이나 공공기관이 웹 인터페이스를 통해 내부 지식 관리 도구를 배포하기 위해 로컬에서 운영되는 LLM을 사용하고자 할 때 다음 사항을 고려해야 함
  - 기업 또는 공공기관의 서버에 LLM을 저장하는 것 자체는 개인정보보호법과 관련이 없으나, AI 시스템은 입력 및 출력과 관련하여 정보주체의 권리를 이행할 수 있어야 함
  - 컨트롤러는 개인정보 공격 및 PII 추출과 같은 개인정보 추출을 방지해야 함\*
    - ※ 구체적으로 LLM 개발자가 제공하는 보안 조치를 구현해야 하며, 개발자의 보호 조치 외에도 책임 당사자는 개인정보 공격 및 PII 추출을 방지하기 위해 필터(filter)와 같은 자체적인 추가 조치를 취해야 함
- (제3자 LLM의 운영 관련) 기업 또는 공공기관은 직원들이 웹 인터페이스를 통해 텍스트 요약을 작성할 수 있도록 애플리케이션 프로그래밍 인터페이스(API)를 통해 LLM을 제공하는 제3자 제공업체와 계약을 체결할 수 있음
  - 이 경우에도 마찬가지로 AI 시스템은 입력 및 출력과 관련하여 정보주체의 권리를 충족할 수 있어야 함

11) GDPR 제12조는 정보주체의 권리 행사를 위한 투명한 정보, 통지 및 형식에 대한 조항을 다룸

- 제공업체를 선택할 때 개인정보 공격 및 PII 추출을 방지하기 위한 보호 조치가 마련되어 있는지 확인하는 것이 중요
- 또한 LLM 운영 전, 책임 소재를 명확히 할 필요가 있음(데이터 처리 대행, 공동 컨트롤러십 또는 독립 컨트롤러십)

### 3. 결론

#### ■ 독일 함부르크 개인정보 감독기관(HmbBfDI)은 LLM이 GDPR이 정의하는 개인정보를 저장하지 않는다고 결론짓고, 기업 및 공공기관의 LLM 도입과 관련한 실무적 시사점을 제시

- HmbBfDI가 발표한 최근 백서는 LLM과 GDPR 간의 관계를 분석하고, LLM이 개인정보를 저장하지 않는다는 결론을 내린 것이 주요 특징
  - 백서는 LLM의 기술적 측면을 상세히 설명하며, 입력된 텍스트가 LLM에서 처리되는 과정에서 개인정보가 숫자 토큰으로 변환된 후 추상화되어 특정 개인과의 직접적인 연결성을 잃는다고 강조
  - 이러한 변환 과정 덕분에 LLM에 저장된 정보는 개별적인 식별자로 기능할 수 없으며, 따라서 LLM이 개인정보를 저장하지 않는다는 결론에 도달
- LLM의 학습 데이터에 개인정보가 포함되어 있더라도, 이는 모델의 학습 과정에서 추상적인 표현으로 변환되므로 GDPR에서 정의하는 개인정보에 해당하지 않음을 강조
  - 모델이 특정 개인정보를 재생산할 가능성이 있다는 점으로부터 발생하는 개인정보 저장 여부 논란에 대해 우연한 LLM의 출력이 곧 개인정보를 저장하고 있다는 증거가 될 수는 없다는 점을 명확히 함
- 또한 LLM의 훈련 과정 중 잠재적인 개인정보보호 위반이 발생하더라도, 이는 모델 사용의 적법성에 영향을 미치지 않으며, 이와 관련된 책임은 오로지 모델 개발자에게 귀속된다는 의견을 제시
- 실무적 시사점으로는 LLM이 개인정보를 저장하고 있지 않더라도 기업과 공공기관이 LLM 사용·운영 시 개인정보의 수집 및 활용을 최소화해야 하는 점과 GDPR을 준수하는 것이 중요하다는 점을 강조

#### 출처 |

1. CJEU, C-319/22, 2023.11.9.
2. CJEU, C-434/16, 2017.12.20.
3. CJEU, C-582/14, 2016.10.16.
4. Datatilsynet, Offentlige myndigheders brug af kunstig intelligens, 2023.10.
5. HmbBfDI, Discussion Paper: Large Language Models and Personal Data, 2024.07.15.
6. HmbBfDI, Hamburger Thesen zum Personenbezug in Large Language Models, 2024.7.15.
7. Vaclav Kosar, Tokenization in Machine Learning Explained, 2022.9.16.

# 구글, 크롬 서드파티 쿠키 지원 종료 계획 철회

- 최신 동향 분석 및 관련 기관 대응 중심으로 -



## [목 차]

### 1. 구글의 서드파티 쿠키 정책 타임라인('20년 폐지 선언~'24년 유지 결정)

### 2. 주요국 관련 규제기관, 협단체 및 광고 업계 반응

- (1) 영국 개인정보 감독기관(ICO)
- (2) 영국 경쟁시장청(CMA)
- (3) 전자 프런티어 재단(EFF)
- (4) 유럽 온라인광고협회(IAB Europe)

### 3. 요약 및 시사점

### 1. 구글의 서드파티 쿠키 정책 타임라인('20년 폐지 선언~'24년 유지 결정)

■ 서드파티 쿠키(Third-party cookie)는 초기 인터넷에서 사용자 선호도와 로그인 정보를 기억하는 등 사용자 경험을 향상시키기 위한 목적으로 도입

- 서드파티 쿠키는 사용자가 현재 방문 중인 웹사이트가 아닌 다른 도메인에서 생성되어 사용자의 브라우저에 저장되는 데이터 파일을 지칭
- 시간이 지나면서 서드파티 쿠키는 광고주들에게 필수적인 도구로 발전하여, 사용자의 온라인 행동을 추적하고 분석하는 데 광범위하게 사용
- 또한 여러 웹사이트에 걸쳐 사용자를 추적하고, 상세한 사용자 프로필을 구축하며 개인화된 광고가 제공되는데 활용되어 디지털 광고의 근간으로 자리매김
- 그러나 개인정보보호 및 프라이버시에 대한 인식이 높아지며, 서드파티 쿠키는 점차 사용자의 기본 권리를 침해하는 기술로 인식되기 시작
- 특히 EU 일반 개인정보보호법(GDPR), CCPA(캘리포니아 소비자 프라이버시법) 등의 개인정보보호 관련 법률 제정으로 인해 쿠키 사용에 대한 규제가 강화되는 추세를 보임
- 일찍이 Safari와 Firefox 등 주요 브라우저들은 기본적으로 서드파티 쿠키를 제한하기 시작하며 업계 변화를 촉구

**표 1 Safari와 Firefox의 서드파티 쿠키 단계적 폐지 타임라인**

날짜	내용
'03년 1월	Safari, Safari 1.0 출시. WebKit의 '기본 쿠키 정책(Default Cookie Policy)'을 통해 서드파티 쿠키 제한 시작
'17년 9월	Safari, Safari 11에서 지능형 추적 방지(Intelligent Tracking Prevention, ITP) 기능을 도입하여 서드파티 쿠키 제한 강화
'19년 9월	Firefox, 향상된 추적 방지(Enhanced Tracking Protection, ETP) 기능을 도입하여 알려진 서드파티 추적 쿠키를 기본적으로 차단하기 시작
'20년 3월	Safari, Storage Access API를 통해 접근하는 경우를 제외하고 모든 서드파티 쿠키를 기본적으로 완전히 차단

## I 구글은 '20년 크롬(Chrome) 웹브라우저에서 서드파티 쿠키를 단계적으로 폐지할 계획을 발표하고 Privacy Sandbox initiative 추진에 착수

- Privacy Sandbox는 개인정보 침해로 논란이 되어 온 서드파티 쿠키를 대체하기 위한 기술 솔루션으로, 사용자 프라이버시를 보호하면서도 효과적인 온라인 광고를 가능하게 하고자 추진
- 구글은 Privacy Sandbox의 일환으로 다음과 같은 기술들을 제안
  - Topics API<sup>12)</sup>: 사용자 개인의 사이트 이용 행태 정보를 추적하지 않으면서도, 방문한 사이트 자체를 분석함으로써 사용자의 일반적인 관심 분야(Topic)를 추론
  - Protected Audience API(구 FLEDGE API): 서드파티에 사용자 정보를 전송하지 않고도 기기에서 광고 입찰 및 송출
  - Attribution Reporting API: 사이트 간 추적에 의존하지 않고도 광고의 효과(예: 매출)를 측정하는 방법을 제공
- 구글의 초기 계획은 '22년 내로 서드파티 쿠키를 지원 종료하는 것이 목적이었으나, 기술적 어려움과 광고 업계의 반발 및 규제기관들의 압박에 직면하자 여러 차례 계획을 연기한 바 있음
  - (경쟁 측면) 영국 경쟁시장청(CMA)는 구글이 디지털 광고 시장에서 불공정한 이점을 얻을 수 있다는 우려에 구글에 대한 공식 조사에 착수한 후, Privacy Sandbox의 기술개발 및 테스트 과정을 면밀히 모니터링<sup>13)</sup>

12) 앞서 구글은 Federated Learning of Cohorts(FLoC)를 제안했었으나, 재식별 가능성 문제가 제기되자 FLoC를 Topics로 대체한 것

13) '21년 1월 7일, CMA는 구글의 경쟁법(Competition Act 1998) 위반 혐의에 대한 조사에 착수. 동 조사는 크롬에서 서드파티 쿠키를 제거하고, 서드파티 쿠키의 기능을 다양한 Privacy Sandbox 도구로 대체하며 핵심 기능을 크롬으로 이전하려는 구글의 계획에 대한 것. CMA는 구글의 이러한 정



- 다만 CMA가 이해관계자들의 테스트 결과를 철저히 검토하기 위해서는 더 많은 시간이 필요했기에, 구글은 '24년 4분기 이후로 서드파티 쿠키 지원 중단 일정을 연장하기로 결정
- (개인정보보호 측면) CMA는 구글의 계획을 검토하는 데 주도적인 역할을 맡고 있으나, 경쟁 관련 이슈와 더불어 개인정보보호 우려도 함께 해결하고자 ICO와 협력
- ICO는 구글의 제3자 쿠키 대체 기술에 대한 지속적인 검토와 우려 표명, 개인정보 친화적인 인터넷 창출 지지, 디지털 광고 업계의 대응 모니터링 등을 통해 개인정보 보호 측면을 적극적으로 감독하며, CMA와 긴밀히 협력하여 구글의 약속 이행과 개인정보 보호 대안 개발을 지속적으로 관리
- 최근 업데이트된 계획대로라면 '25년 2분기까지 모든 크롬 사용자에게 대한 서드파티 쿠키 지원을 100% 중단 예정이었으나, 이는 7월 철회 발표를 기점으로 현재 취소된 상태

**표 2** 크롬 서드파티 쿠키 지원 중단 관련 타임라인

날짜	내용
'20년 1월	구글, 서드파티 쿠키 지원 중단 계획 발표('22년 완료 목표)
'21년 6월	구글, 업계 반발로 서드파티 쿠키 폐지를 '23년 말로 연기
'22년 7월	구글, 서드파티 쿠키 폐지를 '24년 하반기로 재연기
'24년 1월	구글, 전 세계 크롬 사용자의 1%에 대해 서드파티 쿠키 제한 시작
'24년 4월	영국 경쟁시장청(CMA), 구글에 서드파티 쿠키 전면 제거 연기 요청 구글, 완전한 서드파티 쿠키 폐지를 '25년 초로 연기
'24년 7월	구글, 크롬에서 서드파티 지원 중단 계획 철회, 옵트인 모델 전환 계획 발표

**I '24년 7월 22일 구글은 공식 블로그를 통해 크롬 브라우저에서 서드파티 쿠키를 제거하는 대신, 사용자 선택 기반의 옵트인(opt-in) 모델로 전환하겠다고 발표**

- 앤서니 차베스(Anthony Chavez) 구글 Privacy Sandbox 부사장은 블로그를 통해 향후 사용자들이 '웹 브라우징 전반에 걸쳐 정보에 입각한 선택'을 할 수 있을 것이며, 이러한 선택을 언제든지 조정할 수 있을 것이라 언급<sup>14)</sup>

책 변화가 구글에 광고 지출을 집중시켜 디지털 광고 시장의 경쟁을 해칠 수 있다는 우려를 표명. (GOV.UK, Investigation into Google's 'Privacy Sandbox' browser changes, 2024.7.22. 참고)

14) "In light of this, we are proposing an updated approach that elevates user choice. Instead of deprecating third-party cookies, we would introduce a new experience in Chrome that lets people make an informed choice that applies across their web

- 구체적인 추적 방식에 대해서는 언급하지 않았지만, 이로써 크롬에서 서드파티 쿠키가 여전히 사용 가능할 것을 암시
- 한편 서드파티 쿠키 지원 중단 철회 결정은 Privacy Sandbox에 영향을 미치지 않을 예정
  - 구글은 개인정보보호와 유용성을 향상시키는 방향으로 Privacy Sandbox API는 개선하여 계속 제공할 계획이라 언급
- 또한 구글은 크롬의 시크릿 모드에 IP 보호 기능을 도입할 계획임을 밝힘
- 구글은 새로운 접근법에 대해 관련 규제기관들과 논의 중이며, 업계와 협력하여 구현해 나갈 예정이라 밝힘

## 2. 주요국 관련 규제기관, 협단체 및 광고 업계 반응

### (1) 영국 개인정보 감독기관(ICO)

**▮ 그동안 Privacy Sandbox 진행 상황을 면밀히 감시해온 ICO는 구글이 크롬 브라우저에서 서드파티 쿠키를 차단하지 않기로 한 결정에 실망감을 표명(‘24.7.23.)**

- '19년 구글의 샌드박스 프로젝트 시작 시점부터 ICO는 서드파티 쿠키의 차단이 소비자에게 긍정적인 조치가 될 것으로 판단했었음
- ICO는 구글의 새 계획이 ‘중대한 변화’임을 인지하고, 더 자세한 정보가 제공되기 전까지 이에 대한 평가를 보류할 것이라 언급
- 향후 ICO는 이와 관련한 업계 반응을 모니터링하고, 필요시 규제 조치를 고려할 것이라 밝힘

**▮ 한편 ICO는 더욱 프라이버시 친화적인 인터넷 창출을 지원하는 목표를 계속해서 추구할 것이라 발표**

- 또한 디지털 광고 업계가 서드파티 쿠키보다 더 프라이버시 친화적인 대안을 고려할 것을 권장했으며, 불투명한 형태의 추적 행위를 지양할 것을 당부

### (2) 영국 경쟁시장청(CMA)

**▮ CMA는 ICO와 긴밀히 협력하여 구글의 새로운 접근 방식을 신중히 검토할 예정이라 발표**

- 앞서 CMA는 초기 Privacy Sandbox 제안에 대해 ‘구글 생태계에 광고 지출이 더욱 집중되어 경쟁을 왜곡할 수 있다’는 우려를 표명한 바 있음

---

browsing, and they'd be able to adjust that choice at any time. We're discussing this new path with regulators, and will engage with the industry as we roll this out.” (The Privacy Sandbox, A new path for Privacy Sandbox on the web, 2024.7.22. 참고)

- '22년 2월 11일에 구글이 Privacy Sandbox 개발 및 이행과 관련하여 CMA에 구속력 있는 약속<sup>15)</sup>을 한 이후로, CMA는 구글의 약속 준수 여부와 샌드박스 개발 진행 현황에 대한 분기별 보고서를 발행하기 시작
- CMA는 Privacy Sandbox의 경쟁 관련 측면 뿐만 아니라 개인정보보호 측면도 평가하기 위해 ICO와 긴밀히 협력해왔음
- CMA는 구글의 새 접근법이 소비자와 시장에 미칠 수 있는 영향을 모두 고려하고자 8월 12일까지 이해관계자들의 의견을 수렴

### (3) 전자 프론티어 재단(EFF)

Ⅰ 디지털 권리 옹호 비영리 단체 전자 프론티어 재단(Electronic Frontier Foundation)은 구글이 크롬 브라우저에서 서드파티 쿠키 지원 종료 계획을 철회한 것에 대해 매우 비판적인 입장을 취하고 있으며 이를 "약속 파기"라 비난

- EFF는 서드파티 쿠키를 "광범위한 추적 기술"로 규정하며, 이를 통해 기업들이 온라인 활동을 감시하고 맞춤형 광고에 활용한다고 평가
  - 서드파티 쿠키로 인한 수많은 소비자 피해가 여러 해에 걸쳐 기록된 만큼 Safari와 Firefox는 '20년부터 이미 서드파티 쿠키를 차단한 점을 강조
  - 구글의 이번 계획 철회로 인해 수십억 크롬 사용자들이 온라인 감시에 취약한 상태로 남게 되었다고 비판
- 특히 EFF는 구글이 사용자 프라이버시보다 경제적 이익을 우선시한다고 비난
  - 구글 수익의 약 80%가 온라인 광고에서 나오며, 구글이 인터넷에서 가장 큰 사용자 추적자임을 지적
  - 또한, 크롬이 다른 주요 브라우저들에 비해 프라이버시 보호 기능이 부족하다고 비판
- EFF는 서드파티 쿠키를 통해 기업들이 사용자의 상세한 온라인 활동 프로필을 구축할 수 있다고 경고
  - 이같이 수집된 데이터는 보험사, 헤지펀드, 사기꾼, 스톡, 정부기관 등에 판매될 수 있다는 우려를 표명
  - 특히 맞춤형 광고가 취약 계층을 노리는 약탈적 광고나 편향적인 광고를 가능하게 한다고 지적

15) CMA, Case 50972 - Privacy Sandbox Google Commitments Offer, 2022.2.4. 참고 (URL: [https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222\\_Appendix\\_1A\\_Google\\_s\\_final\\_commitments.pdf](https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf))

- 무엇보다 EFF는 경쟁적 시장 조성과 사용자 프라이버시 보호가 양립 가능하다는 입장을 강조
  - 구글의 서드파티 쿠키 지원 유지 결정은 디지털 광고 시장의 경쟁에 대한 광고주들과 규제기관의 우려를 반영한 것
  - EFF는 구글의 서드파티 쿠키 유지 결정이 디지털 광고 시장의 경쟁 우려를 해결하기 위한 잘못된 접근이라고 보고, 이에 대한 대안으로 AMERICA Act\*를 제시
    - \* Advertising Middlemen Endangering Rigorous Internet Competition Accountability (AMERICA) Act: 디지털 광고 시장 경쟁 촉진에 위해 미국에서 초당적으로 발의된 법안으로, 구글이나 메타와 같은 빅테크가 광고 구매 플랫폼과 판매 플랫폼을 동시에 운영하는 것을 금지하는 내용을 담고 있음

## I 구글의 서드파티 쿠키 지원 지속 결정을 고려하여 EFF는 다음과 같은 조치와 제안을 제시

- (구글의 결정 철회 촉구) 타사의 주요 브라우저들이 이미 수년 전부터 서드파티 쿠키를 차단해왔다는 점을 고려할 때, 구글의 이번 결정은 사용자 신뢰는 배반하는 행위라고 비판
  - EFF는 구글이 광고 수익보다 사용자의 프라이버시를 우선시하고, 경쟁 문제에 대한 진정한 해결책을 찾아야 한다고 주장
- (단기적 방안) EFF는 사용자들에게 온라인 개인정보보호 강화 방법으로 Privacy Badger\* 설치를 권장하며, 이는 브라우저 설정이나 정책에만 의존하지 않고 사용자가 침습적 추적으로부터 스스로를 보호할 수 있는 대안책으로 제시
  - \* EFF가 개발한 브라우저 확장 프로그램으로, 서드파티 쿠키와 기타 온라인 추적 기술을 차단하여 온라인 개인정보를 보호
  - 다만, 이는 임시방편에 불과하며 근본적인 해결책이 될 수 없음을 강조
- (장기적 방안) 장기적인 해결책으로는 강력한 프라이버시 법안 마련의 필요성을 강조
  - EFF는 현재 기업들이 서드파티 쿠키 외에도 디지털 핑거프린팅\*, 링크 리다이렉션\*\* 등의 다양한 추적 방식을 활용하고 있기에, 서드파티 쿠키를 차단하는 것 만으로는 충분하지 않을 것이라 지적
    - \* Digital Fingerprinting: 원격 사이트나 서비스가 사용자 기기에 대한 작은 정보들을 수집하여 이를 조합해 사용자 기기의 고유한 '지문'을 생성하는 과정으로, 주로 브라우저를 통해 정보를 수집하는 '브라우저 핑거프린팅'과 설치된 앱을 통해 정보를 수집하는 '기기 핑거프린팅'으로 구분
    - \*\* Link Redirection: 사용자가 웹사이트를 떠나는 링크를 클릭할 때 해당 요청을 추적 서버를 통해 우회시켜, 사용자의 브라우징 행동을 감시하는 기술
  - 이에 따라 사용자의 브라우징 기록을 기본적으로 보호하고, 개인정보를 과도하게 수집하는 행동기반 광고(behavioral ads)를 금지하는 포괄적인 연방 개인정보보호법 제정 필요성을 촉구

#### (4) 유럽 온라인광고협회(IAB Europe)

■ IAB Europe은 구글이 서드파티 쿠키를 완전히 폐지하는 대신 크롬에 새로운 사용자 선택 기능을 도입하기로 한 결정을 인정한 한편, 제한된 기능의 세부 정보 부족으로 인해 이번 발표의 전체적인 영향을 정확히 평가하기 어렵다고 언급

■ 동시에 사용자 경험·경쟁·개인정보보호 표준과의 일치 등 크롬의 새로운 접근방식과 관련한 잠재적 고려사항 및 우려를 다음과 같이 제시

- (기존 표준) 쿠키와 개인정보 처리에 대한 사용자 제어는 이미 GDPR과 ePrivacy 지침 요구사항에 기반한 업계 전반의 표준으로 다루어지고 있음을 지적
- (잠재적 분열) 또한 IAB Europe은 추가적인 선택 단계를 도입함으로써 사용자 경험이 분열될 위험성이 있다 언급
- (경쟁 우려) 구글의 새로운 접근방식이 EU에서 반독점 조사를 받고 있는 애플의 앱 추적 투명성(App Tracking Transparency, ATT)과 유사한 방식으로 퍼블리셔에게 피해를 줄 수 있다는 우려를 표명
  - 애플과 구글이 각 시장(애플: 모바일 앱 생태계, 구글: 웹 브라우징)에서 지배적인 위치를 차지하고 있는 만큼, 구글의 솔루션이 경쟁 문제로 이어져 디지털 광고 생태계의 다른 시장 참여자들에게 불균형적으로 영향을 미칠 수 있다고 지적
- (사용자 인터페이스) 한편 IAB Europe은 크롬의 새로운 사용자 제어방식이 어떻게 구현될지, 기존 Privacy Sandbox API와 어떻게 통합되는지가 중요할 것이라 강조

■ IAB Europe은 구글이 업계 표준 설정 기관들과 긴밀히 협력하여 발표한 새로운 접근방식을 개발하고 업계 피드백을 적극 고려할 것을 촉구

- 동시에 IAB Europe은 과거에 구글이 Privacy Sandbox를 개발하는 과정에서 업계와 협력한 노력을 인정

#### 4. 요약 및 시사점

■ 여러 차례에 걸친 구글의 크롬 브라우저 서드파티 쿠키 정책 변화는 강화되는 개인정보보호 요구와 광고 업계의 실질적 필요 사이에서 균형을 찾으려는 노력을 반영한 것으로 해석

- 반복된 지연과 정책 변경으로 인해 디지털 광고 업계에 불확실성이 커지면서 기업들이 장기적인 전략을 세우는 데 어려움을 초래

- 구글의 새로운 접근방식은 사용자가 크롬에서 개인정보보호 설정을 더욱 잘 제어할 수 있도록 하여 서드파티 쿠키에 대해 정보에 입각한 선택을 할 수 있도록 하는 데 중점을 둠
- 서드파티 쿠키에 대한 지원을 연장하기로 함에 따라 광고주는 맞춤형 광고를 위해 서드파티 쿠키 데이터에 계속 접근할 수 있으며, 적어도 옵트인한 사용자에게 대해서는 현재 수준의 광고 실적 및 수익을 유지할 수 있게 될 전망
  - 다만, 사용자들의 쿠키 차단 선택에 따라 맞춤형 광고의 효율성이 저하되고 비용이 상승하는 효과를 도래할 수 있으며, 특히 크롬의 시장 점유율이 높은 편(60% 이상)임을 고려하면 그 영향이 상당할 것으로 예상
  - 당분간은 서드파티 쿠키가 계속 지원되겠지만 이는 영구적인 해결책이 아니므로 관련 업계는 향후 발생할 수 있는 변화에 계속 대비해야 할 것임
- 또한 Safari 및 Firefox와 같은 다른 브라우저는 이미 타사 쿠키를 차단하고 있기 때문에 디지털 광고 생태계가 더욱 세분화될 가능성이 있어, 개인정보보호 중심 광고 기술에 대한 지속적인 혁신 필요성이 강조

#### **I 구글의 이번 결정으로 인해 사이트 간 추적 관련 개인정보보호 이슈가 지속될 수 있어, 잠재적으로 감독기관들의 더 엄격한 규제 또는 집행조치로 이어질 가능성이 존재**

- 구글이 서드파티 쿠키를 완전히 제거하는 대신 사용자가 직접 관리할 수 있는 시스템을 도입할 것이라는 결정은 사용자에게 더 많은 통제권을 제공하는 한편, 기존의 프라이버시 강화 목표에서 벗어난 결정으로 평가
  - 이로써 서드파티 쿠키를 대체하는 개인정보보호 대안을 개발하고 채택하려는 업계 전반의 노력이 둔화될 우려가 있음
- 규제기관 중 구글 Privacy Sandbox를 면밀히 검토 중이던 ICO는 최근 발표에 대해 부정적인 반응을 보였으나, CMA는 구글의 새로운 접근법에 대한 의견 수렴에 나섬
- 한편, 지난 6월 유럽의 대표적인 개인정보보호 옹호 단체 noyb(None of Your Business)는 오스트리아 개인정보 감독기관에 구글의 Privacy Sandbox의 GDPR 위반 혐의와 관련한 민원을 제기한 상태
  - noyb는 구글이 ▲GDPR의 투명성, 공정성, 정보 제공 요건을 충족하지 못했으며 ▲일반적인 다크패턴을 넘어 동의율을 극대화하기 위한 기만적인 디자인 기법을 사용하고 ▲Privacy Sandbox가 구글 자체의 퍼스트 파티 추적을 가능하게 한다는 사실을 명확히 밝히지 않음으로써 사용자를 오도했다고 주장



- 다만 해당 민원이 제기된 시점은 구글의 최근 발표 이전에 이루어졌기에, noyb와 오스트리아 개인정보 감독기관의 향후 대응은 구글이 서드파티에 대한 수정된 접근법을 구현하는 방식에 따라 달라질 가능성이 있음

## 출처 |

1. Chromium Blog, Potential uses for the Privacy Sandbox, 2019.8.22.
2. Chromium Blog, Building a more private web: A path towards making third party cookies obsolete, 2020.1.14.
3. CMA, Case 50972 &#8211; Privacy Sandbox Google Commitments Offer, 2022.2.4.
4. EFF, Google Breaks Promise to Block Third-Party Cookies, 2024.8.2.
5. Google, Expanding testing for the Privacy Sandbox for the WEb, 2022.7.27.
6. GOV.UK, Investigation into Google's 'Privacy Sandbox' browser changes, 2024.7.22.
7. IAB Europe, IAB Europe Reacts to Google' New Approach to Privacy Sandbox, 2024.7.23.
8. iapp, Google ends third-party cookie phaseout plans, 2024.7.23.
9. ICO, ICO statement in response to Google announcing it will no longer block third party cookies in Chrome, 2024.7.23.
10. Mike Lee, The AMERICA Act: Lee Introduces Bill to Protect Digital Advertising Competition, 2023.3.30.
11. Silicon Republic, Google ends plan to ban third-party cookies on Chrome, 2024.7.23.
12. TechTarget, Adtech, regulators react to Google's third-party cookie reversal, 2024.7.23.
13. The Privacy Sandbox, A new path for Privacy Sandbox on the web, 2024.7.22.
14. 미디어오늘, 구글 쿠키 대란 없던 일로? 언론사 한시름 났다, 2024.7.24.
15. 이코노믹 데일리, 구글, 크롬 서드파티 쿠키 지원 종료 계획 철회, 2024.7.23.

# 2024

## 개인정보보호 월간동향분석

### 발간 목록

No.	호수	제목
1	1월 1호	EU 데이터법(Data Act) 주요 내용 분석 및 시사점
2	1월 2호	EU 내 메타의 무광고 유료 서비스 모델의 개인정보 침해 이슈 분석
3	2월 1호	미국 주(州) 개인정보 보호법에 대한 평가 및 분석
4	2월 2호	DPO 지정 및 역할에 대한 CEA 2023 조사 분석
5	3월 1호	미국 백악관의 정부 데이터 및 민감 개인정보보호를 위한 행정명령 분석
6	3월 2호	EDPB, GDPR 주 사업장에 관한 성명 발표
7	4월 1호	생체인식정보에 대한 개인정보보호 이슈
8	4월 2호	미국 AI 에듀테크 시장 관련 개인정보보호 규제 현황 및 고려사항
9	5월 1호	미국 APRA(American Privacy Rights Act) 주요 내용 분석
10	5월 2호	EDPS 2023 연례보고서 분석
11	6월 1호	중국-미국 간 데이터 관련 이슈
12	6월 2호	EU AI 법 및 GDPR의 상관관계 분석
13	7월 1호	애플의 '애플 인텔리전스' 출시 및 EU 규제 이슈
14	7월 2호	EU 기본권청, DPA의 GDPR 집행 이슈 및 모범사례 공개
15	8월 1호	EU GDPR과 LLM간 관계성 분석
16	8월 2호	구글, 크롬 서드파티 쿠키 지원 종료 계획 철회

# 2024 개인정보보호 월간동향분석

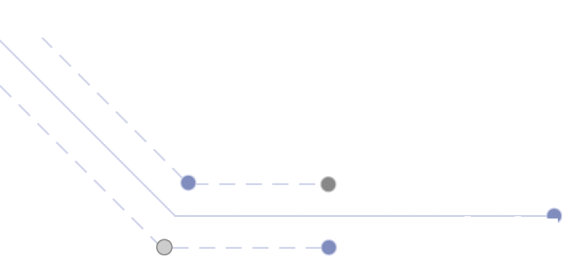
『2024 개인정보보호 월간동향분석 보고서』는  
개인정보보호위원회 출연금으로 수행한  
사업의 결과물입니다.

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

본 보고서의 내용은  
한국인터넷진흥원의 공식 견해가 아님을 알려드립니다.

## 발행

**발행일** 2024년 9월  
**발행처** 한국인터넷진흥원 개인정보제도팀  
전라남도 나주시 진흥길 9  
Tel : 061-820-1231



# 2024 개인정보보호 월간동향분석

2024 Vol.8

## PRiVACY REPORT

