

# PRiVACY REPORT

## 개인정보보호 월간동향분석

2024년 11월호



## | CONTENTS |

2024년 11월호

1

EU 법제상 AI 시스템 배포자의  
DPIA 주요 검토사항

2

영국 데이터(사용 및 접근) 법(안) 주요 개정 사항 분석

3

영국 ICO, CMA, 온라인 선택 아키텍처의  
유해한 설계 사례와 개인정보 악영향 고찰

# EU 법제상 AI 시스템 배포자의 DPIA 주요 검토사항



## [목 차]

### 1. 개요

### 2. DPIA 관련 주요 검토사항

- (1) 1단계: 처리 작업에 대한 설명
- (2) 2단계: 필요성 및 비례성 평가
- (3) 3단계: 정보주체의 권리와 자유에 대한 위험성 평가
- (4) 4단계: 위험 완화 조치

### 3. 결론 및 시사점

### 1. 개요

■ 개인정보 영향평가(DPIA, Data Protection Impact Assessment)는 고위험 AI 시스템의 투명성, 안전성, 및 책임성을 강화하기 위한 핵심 도구로, EU 일반 개인정보보호법(GDPR)과 EU AI법 (Artificial Intelligence Act)에 의해 그 중요성이 강조되고 있음

- 개인정보보호와 AI 기술의 책임 있는 사용이 점차 중요해지는 환경 속에서, DPIA는 개인의 권리와 자유를 보호하고 AI 시스템의 신뢰성을 확보하는 필수적인 역할을 담당함
- GDPR 제35조는 ▲대규모의 민감 정보 처리 ▲자동화된 개인별 의사결정 ▲공공장소의 대규모 모니터링과 같은 고위험 처리 상황에서 DPIA를 의무화하고 있음
  - 이와 함께, EU AI법 제26조는 고위험 AI 시스템을 배포하는 조직(이하 "배포자")이 개인정보를 처리할 때 DPIA 수행을 요구하며, 시스템 설계와 사용에 있어 법적 및 윤리적 기준 준수를 명시함.
- 고위험 AI 시스템은 채용, 직원 관리, 성과 평가와 같은 조직 운영에 직접적으로 활용될 수 있으며, 이러한 사용 사례는 EU AI법이 규정하는 높은 위험 수준에 해당될 가능성이 있음
  - DPIA는 이러한 시스템이 초래할 잠재적 위험을 사전에 식별하고 이를 완화하기 위한 핵심 절차로 자리 잡고 있음
  - 특히, 배포자는 DPIA를 통해 개인정보 처리의 목적과 방식을 정의하며 컨트롤러로서의 역할을 수행하게 됨
  - EU AI법 제26조제(3)항은 배포자가 입력 데이터를 통제하는 경우, 해당 데이터가 시스템 목적에

적합하고 충분히 대표성을 가져야 한다고 규정함

- 배포자가 AI 시스템 출력물(예: 예측, 분류)에 영향을 미치는 경우에도, GDPR 및 EU AI법에 따라 컨트롤러로 간주되어 DPIA 수행 의무가 발생함

**I 결론적으로, DPIA는 AI 시스템 설계 및 운영에서 잠재적 위험을 관리하고, 개인의 권리를 보호하며, 기술 신뢰성을 높이는 필수 도구로 자리 잡고 있음**

- GDPR과 EU AI법의 상호 보완적인 요구사항은 DPIA의 중요성을 더욱 부각시키며, AI 시스템의 책임 있는 배포와 사용을 촉진하고 있음
- 이에 본고는 GDPR과 EU AI법의 연계성을 중심으로, 고위험 AI 시스템에 대한 DPIA의 중요성과 배포자가 수행해야 할 위험 평가 및 완화 조치에 대해 다루고자 함

## 2. DPIA 관련 주요 검토사항

### (1) 1단계: 처리 작업에 대한 설명

**I DPIA 수행 절차의 첫 번째 요소는 고위험 AI 시스템의 처리 작업에 대한 설명으로, 여기에는 해당 AI 시스템의 처리 목적과 (해당 시) 컨트롤러의 정당한 이익이 포함**

- 이는 배포자가 AI 시스템의 결과물(output)을 해석하고 적절히 사용할 수 있도록 하여 투명성을 보장하기 위함임
  - EU AI법 제13조제(2)항은 사용설명서 제공을 제공자(provider)의 의무사항으로 규정하고 있으며, 처리 작업은 사용설명서를 참조하여 상세히 설명되어야 함
- 사용설명서는 간결하고 명확하게 작성되어야 하며, 아래와 같은 요소들을 포함해야 함

**표 1 AI 시스템 사용설명서 구성 요소**

항목	세부 내용
제공자의 식별정보 및 연락처	- AI 시스템 제공자의 이름 및 연락처 정보 포함
AI 시스템의 주요 특징	- 의도된 목적: 시스템의 주요 사용 목적을 명시
	- 정확성, 견고성, 사이버보안 수준: 측정 가능한 지표를 포함하여 기술
	- 건강, 안전, 기본권에 대한 위험: 알려진 또는 예상되는 위험을 서술
	- 결과물의 설명 가능성: 가능하다면, 결과물의 설명 논리를 포함

	<ul style="list-style-type: none"> <li>- 특정 대상에 대한 성능: 시스템이 사용되도록 설계된 특정 대상에서의 성능 명시</li> <li>- 입력 데이터의 세부 정보: 입력 데이터의 특성과 출처에 대한 정보 포함</li> <li>- 결과물의 해석 및 적절한 사용을 지원하는 정보</li> </ul>
적합성 평가 과정에서의 변경사항	<ul style="list-style-type: none"> <li>- 제공자가 적합성 평가 중 발견한 AI 시스템 및 성능의 변경사항 포함</li> </ul>
인적 감시 및 기술적 조치	<ul style="list-style-type: none"> <li>- 결과물 해석을 지원하기 위한 기술적 조치 및 인적 감시 방안 포함</li> </ul>
컴퓨팅 및 하드웨어 자원	<ul style="list-style-type: none"> <li>- 필요한 자원, 예상 사용 기간, 유지 관리 및 관리 조치에 대한 정보 포함</li> </ul>
로그 관리 메커니즘	<ul style="list-style-type: none"> <li>- 로그 데이터를 수집, 저장 및 해석하는 메커니즘 포함</li> </ul>

- 배포자는 AI 시스템의 개인정보 처리와 관련하여 처리 목적과 법적 근거 외에도 다음 사항을 명확히 기술해야 함
  - 처리되는 개인정보의 종류
  - 정보주체의 범주
  - 개인정보의 출처
  - 정보주체가 해당 처리를 예상할 가능성
- 데이터 흐름 및 처리 단계 식별과 관련하여 영국 개인정보 감독기관(ICO, Information Commissioner's Office)의 '['23년 가이드라인](#)'\*을 참고할 수 있음
  - \* ICO의 '23년 AI와 개인정보보호 가이드라인(Guidance on AI and data protection)은 AI 시스템에서 컨트롤러와 프로세서를 구분하는 상황을 명확히 설명하며, DPIA 수행에 있어 배포의 역할을 구체화함
  - 해당 가이드라인에 따르면, DPIA는 GDPR 제22조에 근거하여 데이터 흐름과 AI 시스템의 작동 단계에서 발생할 수 있는 개인에 대한 영향을 명확히 구분해야 함
  - 구체적으로, DPIA는 의사결정 과정에서 인간이 개입하는 정도를 식별 및 기록해야 하며, 잘못된 자동화된 결정을 수정할 수 있는 인적 검토 프로세스를 마련하는 것이 필요함
  - AI 시스템의 복잡성은 그 처리 활동에 대한 설명을 어렵게 만들 수 있기에, ICO는 처리 활동 설명을 크게 ▲기술적 설명\* ▲일반적 설명\*\*, 총 두 가지 버전의 설명을 유지할 것을 권장함
  - \* 전문가를 대상으로 AI 시스템의 처리 방식 및 세부적인 기술적 내용을 포함하는 심층적인 정보를 제공하기 위한 것
  - \*\* 정보주체를 대상으로 AI 시스템의 처리 방식과 기본 논리를 이해하기 쉽게 서술하여 접근성을 높이기 위한 것

## (2) 2단계: 필요성 및 비례성 평가

■ DPIA의 두 번째 핵심 요소인 필요성 평가(necessity assessment)는 AI 시스템의 도입 및 활용이 조직의 목표 달성을 위해 필수적임을 입증하는 절차로, 대안이 없음을 명확히 하는 것을 포함함

- 필요성의 평가는 대안 분석과 명확한 근거 제시를 기준으로 함
  - 즉, 동일한 목표(예: 처리 효율성, 시간 및 비용 절감 등)를 달성할 수 있으면서도 덜 침해적인 방법이 없는지 검토해야 하며, 고위험 AI 시스템 사용의 불가피성을 명확한 근거를 통해 증명해야 함

■ 또한, DPIA는 AI 시스템이 개인정보를 처리하는 과정이 비례성 원칙(proportionality)에 부합하는지 평가할 수 있는 체계를 제공하며, 이 과정에서 고려해야 할 사항은 다음과 같음

- (잠재적 피해 분석) AI 시스템 사용으로 인해 개인에게 발생할 수 있는 잠재적 해악 평가
- (인간과 AI 비교) AI가 인간의 의사결정을 보완하거나 대체하는 경우, 인간과 알고리즘의 정확도를 비교하여 AI 사용의 정당성 문서화
- (개인정보 처리 기대치) 정보주체가 해당 개인정보 처리를 합리적으로 예상할 수 있도록 개인정보 처리방침을 안내하는 등의 방법으로 충분한 정보 제공

■ AI 시스템의 통계적 정확성은 데이터 최소화 원칙과 균형을 이루어야 함

- ICO 가이드라인에서 소개한 예시에 따르면, 이력서(CV) 스크리닝 톨과 같은 AI 시스템이 구직자 평가를 위해 광범위한 개인정보를 요구하는 경우, 시스템 배포자는 해당 개인정보 수집의 정당성을 우선적으로 평가해야 함
  - 이와 같은 사례에서, AI 시스템의 성능 오류가 크게 감소하여 통계적 정확성이 향상된다면 추가적인 데이터 처리의 정당성이 인정될 가능성이 있음
  - 반면, 정당성이 입증되지 않을 경우, 다른 AI 또는 소프트웨어와의 통합 변경 등 시스템 수정 방안을 검토하거나 대체 제공업체를 고려해야 함

## (3) 3단계: 정보주체의 권리와 자유에 대한 위험성 평가

■ DPIA의 세 번째 핵심 요소는 정보주체의 권리 및 자유에 대한 위험성 평가로, 이는 앞서 수행된 필요성 및 비례성 평가 결과를 토대로 실시함

- EU AI법 제27조에 근거하여 특정 배포자들은 고위험 AI 시스템에 대해 기본권 영향평가(FRIA, Fundamental Rights Impact Assessment)를 수행해야 함

- 배포자 중 ▲공공기관 또는 공공 서비스를 제공하는 민간 기관 ▲개인의 신용도를 평가하는 기관 ▲생명보험 또는 건강보험의 위험도나 가격을 산정하는 기관이 이러한 의무 이행 대상자에 해당함
- FRIA의 목적은 고위험 AI 시스템이 기본권에 미치는 영향을 구체적으로 평가하는 것으로, ▲인간의 존엄성 ▲사생활 및 가족생활 존중 ▲표현의 자유 및 정보의 자유 ▲소비자 보호 ▲근로자의 권리 등이 대표적인 평가요소임
- EU AI법 27조제(4)항에 의거하여 FRIA는 DPIA를 보완하는 역할을 할 수 있음
- 권리 및 자유 위험성 평가를 위해 배포자는 (고위험) AI 시스템이 개인에게 미칠 수 있는 위험을 식별하고, 그 발생 가능성과 심각도에 근거하여 점수를 부여해야 함
  - 배포자가 정당한 이익(legitimate interest)을 법적 근거로 사용하는 경우, 3단계 테스트(목적, 필요성, 균형성) 참조
- AI 시스템 배포 단계에서 고려해야 할 권리 및 자유에 대한 주요 위험을 식별하는 데 있어, 독일 바이에른 주 개인정보 감독기관(BayLDA, Bayerisches Landesamt für Datenschutzaufsicht)이 공개한 '['24년 가이드라인](#)'을 참고할 수 있음
- 해당 가이드라인은 권리와 자유에 대한 잠재적 위험 목록을 포함하고 있으며, 그 중 AI 시스템 배포 단계에 적용될 수 있는 주요 위험은 다음과 같음

**표 2** BayLDA 가이드라인 - AI 시스템 배포 단계 주요 위험

위험	예시
왜곡 및 편향 존재	- 예: 인사 관련 의사결정에서의 성별 편향
차별적/혐오적 결과물 산출	- 예: 종교와 관련된 차별
설명 가능성/투명성 부족	- 예: 차별적 진술의 데이터 출처가 불분명한 경우
인간의 통제 옵션 기능 미흡	- 예: AI 출력을 후속 처리 과정에 지나치게 무비판적으로 채택한 경우
AI 시스템의 부적절한 보안	- 예: 사이버 범죄자가 AI 모델에 백도어(backdoor)를 설치하거나 훈련 데이터를 조작할 수 있는 가능성
AI 시스템 배포자의 인식 부족	- 예: 충분한 정보권 없이 AI 시스템을 사용한 경우
정보주체 권리 보호 미흡	- 예: 불충분한 로깅(logging)으로 인한 문제

#### (4) 4단계: 위험 완화 조치

■ DPIA의 마지막 요소는 개인정보보호를 위한 위험 완화 조치로, ▲안전조치(safeguards) ▲메커니즘(mechanisms) ▲보안조치(securiy measures) 등을 포함

- 배포자는 앞서 식별된 각 위험에 대해 추가적인 위험 감소 방안을 고려해야 함
  - EU AI법 제4조 및 제26조제(2)항에 근거한 AI 리터러시(AI literacy)는 AI 시스템의 배포 및 모니터링 책임 이행자에게 핵심적인 요소
  - 관련 직원은 (고위험) AI 시스템을 감독하고, 인적 오류를 최소화하며, 의미 있는 참여와 검토를 강화할 수 있도록 적절한 교육을 이수해야 함
- DPIA는 AI 시스템의 보안을 강화하고 정확성을 확보하기 위한 기술적 및 조직적 조치를 문서화해야 함
- CNIL 가이드라인은 이러한 기술적 및 조직적 조치에 대한 권장 목록을 제공하고 있으며, 특히, 배포 단계에서 고려해야 할 주요 조치는 다음과 같음
  - (개인정보 최소화 조치) 처리 활동의 옵트아웃(opt-out) 가능성 제공 및 정보 보유 기간 단축
  - (가명화 및 익명화) 데이터 마스킹 및 삭제(redaction) 절차를 포함한 가명화 및 익명화 기법 적용
  - (설명 가능성이 큰 AI 시스템 사용) 결과물의 설명 가능성을 높이는 AI 시스템 채택을 통한 투명성 확보
  - (정기적인 AI 시스템 평가) 비준수 영역을 식별 및 개선하기 위한 정기적 평가 실시
  - (제3자 및 하청업체의 접근 제한 및 통제) 외부 사용자 및 하청업체의 접근 엄격히 관리 및 통제
  - (정보주체 요청 처리 메커니즘) GDPR 제15조(접근권) 등 정보주체 요청에 대응하기 위한 로그 사용 등 내장 메커니즘 마련
  - (다기능 위원회 구성) EU AI법 제26조제(5)항에 근거해 AI 시스템의 운영을 모니터링하는 다기능(cross-functional) 위원회를 설립하여 지속적인 관리 체계 구축
- GDPR 제35조제(2)항에 의거하여, 배포자는 기존 위험을 완화하거나 회피하기 위해 개인정보보호책임자(DPO, Data Protection Officer)와 협의해야 함
  - DPO는 AI 구현 프로젝트 초기 단계부터 참여해야 하며, 프로젝트 팀과 DPO간 명확하고 개방적인 의사소통 채널을 구축하여 초기 단계에서 위험을 식별하고 해결할 수 있어야 함
- 또한, GDPR 제35조제(9)항에 따라 배포자는 정보주체 또는 그 대리인의 의견을 수렴하고 이를 기록할 의무 발생



- 다만, 상업적 이익이나 처리의 보안과 같은 정당한 사유가 있는 경우에는 예외가 인정될 수 있음
- 배포주가 고용주인 경우, EU AI법 제26조제(7)항에 의해 영향받는 근로자와 그 대표자를 필수적으로 포함
- 배포자는 위와 같이 DPIA의 각 단계를 진행하고 위험 수준을 결정한 후, 위험 완화 조치를 적용하여 처리와 연관된 잠재적 위험 식별
  - 모든 위험을 제거할 법적 의무는 없으나, 각 위험을 ▲제거 ▲감소 ▲수용 등으로 체계적 분류 요구
  - 만약 개인의 개인정보보호 권리에 대한 고위험 요소 지속 시, 개인정보 처리를 개시하기에 앞서 관할 개인정보 감독기관과 사전협의 진행

**표 3** DPIA의 핵심 구성 요소 정리

항목	주요 내용
처리 활동에 대한 설명	- 처리 활동, 필요성/비례성 평가, 권리 기반 위험 평가, 기술적 및 조직적 조치 목록 포함
위험 완화 이후의 잔여 위험 수준	- 위험 완화 조치가 시행된 후 잔여 위험 수준에 대한 전체적 평가
이해관계자 협의	- DPO, 정보주체(또는 그 대리인), 공동 컨트롤러, (해당할 경우) 프로세서와의 협의 내용 문서화
감독기관 협의 여부 결정	- 개인정보 감독기관과의 사전 협의 필요 여부에 대한 결정 포함

- 배포자는 DPIA는 지속적으로 관리 및 갱신이 필요한 문서로 인식해야 하며, 다음과 같은 상황 발생 시 재평가를 실시해야 함
  - 처리 목적이 변경되는 경우.
  - 정보주체에게 가해지는 위험 양상이 변화하는 경우
  - 조직의 비즈니스 또는 사회적 환경에 변동이 생기는 경우
- 위 내용을 바탕으로, EU AI법 제26조의 적용을 받는 배포자는 다음 의무를 수행해야 함
  - 사용 중인 AI 시스템 목록화 및 위험 수준 지정
  - 고위험 AI 시스템의 경우, 필요한 위험평가(DPIA 또는 FRISA) 유형을 결정할 것
  - 위험평가를 수행하고 위험 완화 조치를 식별할 것
  - AI 시스템 배포에 관여하는 직원들을 대상으로 교육할 것

- 위험의 지속적 모니터링 체계를 구축할 것

### 3. 결론 및 시사점

#### ■ EU AI법과 GDPR의 상호작용은 AI 기술의 발전 속에서 데이터 보호의 포괄적 접근 필요성을 강조함

- 특히, 고위험 AI 시스템에 대한 엄격한 DPIA 수행은 개인의 권리와 자유에 대한 잠재적 위험을 평가하고 완화하는 데 필수적임
- AI 시스템 배포자는 두 규제를 준수함으로써 단순히 법적 의무를 충족하는 것을 넘어, 투명성, 공정성, 그리고 책임성을 기반으로 한 AI 기술의 신뢰성을 제고할 수 있음
- AI 기술이 지속적으로 진화함에 따라, 배포자는 동적이고 대응 가능한 DPIA 체계를 유지해야 하며, 이를 통해 새로운 과제에 유연하게 대응하고 데이터 주체의 권리를 보호해야 함
- 또한, AI 시스템의 지속적 모니터링과 관련 이해관계자와의 협력을 통해, 높은 수준의 개인정보보호 및 윤리적 AI 사용 기준을 유지하는 것이 중요함

#### 출처 |

1. BayLDA, KI & Datenschutz: Datenschutzfolgenabschätzung
2. CNIL, Carrying out a data protection impact assessment if necessary, 2024.6.7.
3. CNIL, IA : Réaliser une analyse d'impact si nécessaire, 2024.4.8.
4. Dataguidance, EU: The AI Act meets GDPR - The particular case around DPIAs by deployers, 2024.10.9.
5. ICO, Guidance on AI and Data Protection, 2023.3.15.

# 영국 데이터(사용 및 접근) 법(안) 주요 개정 사항 분석



## [목 차]

### 1. 개요

### 2. 법안 분석

- (1) UK GDPR 개정
  - 1) 과학적 연구에 대한 정의 및 연구에 대한 광범위한 동의 규정 도입
  - 2) 개인정보 처리 적법성 근거 추가 및 명확화
  - 3) 목적 제한 원칙 완화
  - 4) 특수 범주 개인정보 관련 추가 권한
  - 5) 접근권 행사에 대한 컨트롤러의 대응 방식 명확화
  - 6) 자동화된 의사결정 사용 제약 완화
  - 7) 개인정보 국외이전 시 적정성 평가 방법 대체 : 개인정보보호 테스트
- (2) DPA 2018 개정
  - 1) ICO 개편
  - 2) 민원 제기 메커니즘 변경
- (3) PECR 2003 개정
  - 1) 쿠키 수집 관련 동의 요건 완화
  - 2) 과징금 상향
- (4) 기타 제도 개선

### 3. 기타 사항

### 1. 개요

#### ■ 영국 정부는 2024년 10월 23일 데이터(이용 및 접근) 법(안)(Data (Use and Access) Bill)을 발표하고 이를 상원(House of Lords)에 제출

- 이번 법안은 직전 의회가 2024년 5월 해산되면서 폐기되었던 데이터 개혁 법안인 개인정보보호 및 디지털 정보 법(안)(Data Protection and Digital Information Bill)을 기반으로 일정 부분 수정을 가한 법안
- 정부는 이번 법안 제안을 통해 영국의 데이터 관리, 개인정보보호, 디지털 전환에 대한 전략적 혁신을 바탕으로 산업 부문 전반에 걸쳐 데이터의 잠재력을 끌어내고, 이와 동시에 규제

명확성을 높이고자 함

- 즉, 동 법안은 영국의 개인정보보호 제도 개혁을 추구함과 동시에, 영국의 경제 성장, 공공 서비스 개선, 국민의 편리한 삶을 위한 데이터의 효율적인 이용 촉진 등 데이터의 전반적인 활용 측면 등을 강조

## Ⅰ 이번 법안은 기존 개인정보보호 관련 법령 개정을 중점적으로 다루면서도, 관련 법률 개정 · 데이터 활용 관련 신규 제도 도입 등을 바탕으로 한 광범위한 개선사항을 포함

- 법안은 하나의 법안 아래에 ▲영국 일반 개인정보보호법(이하 UK GDPR) ▲2018년 개인정보보호법(Data Protection Act 2018(이하 DPA 2018)) ▲2003년 개인정보보호 및 전자통신 규정(Privacy and Electronic Communications (EC Directive) Regulations 2003 (이하 PECR 2003) 등 영국의 개인정보보호 관련 법령에 다수의 조항을 개정 및 신설하고 부칙(Schedule) 등을 추가 및 대체하는 등 개인정보보호 제도 개혁을 위한 폭넓은 법률 개정을 추진
- 이외에, 보건 데이터 표준 확립, 스마트 데이터, 디지털 검증 서비스 제도 등 데이터 활용에 관한 신규 프레임워크 등도 도입
- 다만, 이번 법안은 이전 법안에서 많은 비판을 받았던 쟁점조항을 다수 제외시키면서 논란을 최소화하는 등 의회 통과를 위한 강력한 의지를 반영
  - 이 같은 접근 방식은 데이터 개혁 추진과 별개로 2025년 있을 EU집행위원회의 영국에 대한 적정성 결정(adequacy decision)<sup>1)</sup> 재평가에서 EU에 대한 영국의 적정성 지위를 지속 유지하기 위한 조치로 해석

## 2. 법안 분석

### (1) UK GDPR 개정

#### 1) 과학적 연구에 대한 정의 및 연구에 대한 광범위한 동의 규정 도입

Ⅰ 법안은 연구를 수행하는 조직으로부터 연구와 관련한 규정이 너무 제한적이라는 비판 제기를 수용, UK GDPR 제4조에 과학적 연구 목적 개인정보 처리에 관한 정의를 추가함으로써 과학적 연구 목적의 의미를 명확히 함과 동시에 그 범위를 확장

- 동 법안에서 과학적 연구 목적의 개인정보 처리는 공적 또는 사적 자금 지원 여부, 상업적 또는 비상업적 활동으로 수행되는지 여부와 관계없이 합리적으로 과학적이라고 설명할 수 있는 모든

1) 개인정보보호 수준이 EU와 동등한 수준으로 인정될 경우 기업이 별도의 조치 없이 개인정보 국외이전을 할 수 있도록 허용하는 것으로 EU 집행위원회가 결정 권한을 가짐

연구 목적의 처리를 의미

- 예컨대, 사적으로 자금을 조달받는 상업 활동이나 기술 개발을 위해 이루어지는 개인정보 처리라도 해당 활동을 과학적이라고 합리적으로 설명할 수 있는 한 과학적 연구에 해당

## Ⅰ 또한 동 조항에 과학적 연구에 대한 정보주체의 동의 관련 규정을 신설하여 과학적 연구에서의 컨트롤러의 동의 획득 요건을 일부 완화

- 정보주체가 과학적 연구에 대한 동의를 제공할 당시 모든 연구 목적을 파악할 수 없더라도 정보주체는 여러 유형의 과학적 연구에 개인정보가 활용되는 데 동의를 제공할 수 있음

## 2) 개인정보 처리 적법성 근거 추가 및 명확화

### Ⅰ 법안은 개인정보 처리 적법성의 근거로서, '인정된(recognised)' 정당한 이익 목적을 UK GDPR 제6조 제1항제(ea)호에 추가하고 그 구체적인 사항을 별표1(Annex 1)에 열거

- 동 열거된 정당한 이익은 ▲국가 안보, 공공 안전 및 방위 ▲비상 사태 대응 ▲범죄 탐지, 조사, 예방 및 범죄자 체포, 기소 ▲취약 계층 보호 등으로, 주로 다양한 공공의 이익을 목적으로 함
  - 인정된 정당한 이익 목적을 가진 개인정보 처리와 관련해 적법성을 평가할 경우에는 컨트롤러의 정당한 이익 대비 정보주체의 권리 및 이익 간 비교 형량을 거칠 필요가 없음
- 과학혁신기술부(Secretary of State for Science, Innovation and Technology) 장관은 인정된 정당한 이익 목적으로 볼 수 있는 기타 유형을 별표에 추가하는 방식으로 해당 목록을 변경할 수 있음

### Ⅰ 법안은 또한 UK GDPR 제6조제1항제(f)호의 기존 정당한 이익 목적에 해당하는 처리의 유형을, 조항을 추가하여 상세화

- 법안은 동법 제6조 내에 제11항을 신설하여, 동조제1항제(f)호의 정당한 이익 목적 처리 유형으로서 ▲직접 마케팅 목적을 위해 필요한 처리 ▲내부 관리 목적으로서 조직 내 개인정보 이전(고객, 직원 또는 기타사항 관련) ▲네트워크 및 정보 시스템의 보안 보장 목적을 위해 필요한 처리 등을 제시
  - 이는 기업이 개인정보를 처리하는 근거로 정당한 이익 목적을 들고자 할 때 기업에 보다 명확성과 편의를 제공하기 위함

## 3) 목적 제한 원칙 완화

### Ⅰ 법안은 UK GDPR 제5조 대원칙 중 하나인 목적 제한 원칙을 완화하기 위해 제8A조를 신설, 목적

**범위 내에서 책임감 있게 개인정보를 활용하려는 조직에 명확성을 제공하고 원활한 법률 준수 활동을 지원하고자 함**

- 신설 조항은 새로운 처리 목적이 기존 처리 목적과 호환되는지 여부를 컨트롤러가 용이하게 판단할 수 있도록 기준 및 방법을 규정
  - 구체적으로 컨트롤러는 목적의 호환 여부를 검토할 때 ▲원래 목적과 새로운 목적 사이의 연관성 ▲정보주체와 컨트롤러 간의 관계를 고려하여 개인정보가 수집된 맥락 ▲특수 범주 개인정보 또는 범죄 관련 개인정보 등 처리의 성격 ▲개인정보 처리가 정보주체에게 미칠 수 있는 결과 ▲적절한 보호조치(예: 암호화 또는 가명화)의 존재 여부 등을 고려해야 함
  - 더불어, 기타 특정 상황(▲연구, 아카이빙, 통계 목적 ▲공공 보안 ▲비상 사태 대응 ▲범죄 탐지, 조사, 예방 및 범죄자 체포, 기소 ▲정보주체 및 타인의 중대한 이익 보호 ▲취약 계층 보호 ▲세금 부과 또는 징수 ▲법적 의무 또는 법원/재판소 명령 준수 등)에서는 새로운 목적이 기존 처리 목적과 호환되는 것으로 별표2(Annex 2)에 규정하고, 과학혁신기술부장관에게 호환성이 간주되는 해당 목록을 수정할 수 있는 권한을 부여

#### **4) 특수 범주 개인정보 추가 권한**

**Ⅰ 법안은 UK GDPR 제11A조를 신설하여 과학혁신기술부 장관으로 하여금 동법 제9조 이외에 새로운 특수 범주 개인정보를 추가할 수 있는 하위규정(regulation) 제정 권한을 부여**

- 과학혁신기술부 장관은 하위규정을 통해 특수 범주 개인정보를 추가하여, 해당 유형의 개인정보가 UK GDPR 제9조제1항의 처리 금지 조항의 적용을 받도록 규정하거나 또는 적용받지 않도록 규정하는 것이 가능하며,
- 동조 제2항의 처리 금지 예외가 적용되거나 적용되지 않도록 규정하는 것 또한 가능
- 과학혁신기술부 장관은 하위규정에 나열된 특수 범주 개인정보의 일부를 삭제할 수 있음
  - 단, 이 권한은 UK GDPR 제9조에 명시된 기존 특수 범주 개인정보를 제거하는 데에 행사될 수는 없음

#### **5) 접근권 행사에 대한 컨트롤러의 대응 방식 명확화**

**Ⅰ 법안은 UK GDPR 제12A조를 신설하여 정보주체가 동법 제15조에 따른 접근권 행사 시 컨트롤러로 하여금 특정 요건 하에서 추가 정보 제공을 요청할 수 있는 권한을 부여**

- 컨트롤러가 UK GDPR 제15조에 따른 정보주체의 접근권 행사에 대응하기 위해 합리적으로 추가 정보가 필요한 경우 컨트롤러는 정보주체에게 추가 정보를 제공하도록 요청할 수 있음
  - 대표적인 예로 컨트롤러가 정보주체에 관한 대량의 정보를 처리하는 경우가 이에 해당

## Ⅰ 또한 법안은 동법 제12조 개정 및 제15조제1A항 신설을 통해 접근권 행사에 대응한 컨트롤러의 정보 검색 노력 정도 및 응답 기한 관련 기존 가이드라인을 법률에 도입

- 컨트롤러는 합리적이고 비례적인 검색(reasonable and proportionate search)을 통한 정보 제공만으로 정보주체의 접근권 행사를 충족시킬 수 있음
- 다만, 정보 제공은 지체 없이(without undue delay) 그리고 어떠한 경우에도 요청을 받은 후 한 달 이내에 수행되어야 함 (단, 기한 연장이 가능한 특수한 예외 존재)

## 6) 자동화된 의사결정 사용 제약 완화

### Ⅰ 법안은 자동화된 의사결정 수단을 활용하기 전 개인정보 처리의 적법성을 갖추도록 한 현 UK GDPR 제22조의 요건을 대폭 제거

- 이는 특히 AI 시스템을 사용하는 조직이 EU GDPR보다 더 광범위하게 자동화된 의사결정 수단을 활용할 수 있도록 허용하는 조치
- 다만 GDPR 제9조의 특수 범주 개인정보 처리와 관련된 자동화된 의사결정 수단 사용에서는 최소한의 제한이 여전히 존재
  - 즉, 민감한 개인정보 처리를 위해 자동화된 의사결정 수단을 사용하는 경우 반드시 정보주체의 명시적인 동의가 있거나, 의사결정이 정보주체와 컨트롤러 간의 계약 체결 또는 계약 이행에 필요하거나, 또는 의사결정이 법률로써 요구 또는 승인된 경우라야 함

## 7) 개인정보 국외이전 시 적정성 평가 방법 대체 : 개인정보보호 테스트

### Ⅰ 법안은 EU GDPR 체제로부터 이어져 왔던 제3국 및 국제조직의 개인정보보호 적정성 평가 방식인 적정성 결정(adequacy decision) 대신 영국 색채가 강한 개인정보보호 테스트(data protection test) 제도를 도입

- 법안은 UK GDPR 제45조를 개정하여 개인정보 수신지 국가의 개인정보보호 기준이 영국의 보호 기준보다 '실질적으로 낮지 않음(not materially lower)'을 증명하면 되도록 함
  - 이를 통해 기존 EU GDPR 체제에서의 적정성 결정 요건이었던 '본질적으로 동등(essentially equivalent)할 것'을 대체하고 그 임계치를 낮춤
- 개인정보보호 테스트 통과 여부를 판단할 때는 ▲개인정보 수신지 국가의 법치, 인권존중 ▲개인정보 감독기관의 존재 및 권한 ▲정보주체의 사법적 또는 비사법적 구제 조치 구비 여부 ▲수신지 국가의 개인정보 국외이전 규정 존재 여부 ▲수신지 국가의 국제적 의무 및 헌법, 전통 및 문화 등을 종합적으로 판단하도록 함

**표 1 데이터(사용 및 접근) 법(안)의 UK GDPR 관련 개정 요약**

구분	내용	UK GDPR 조항
과학적 연구에 대한 정의 및 연구에 대한 광범위한 동의 규정 도입	<ul style="list-style-type: none"> <li>과학적 연구 목적의 의미 명확화 및 연구 범위 확장</li> <li>과학적 연구에서의 컨트롤러의 정보주체에 대한 동의 획득 요건 완화</li> </ul>	<ul style="list-style-type: none"> <li>제4조</li> </ul>
처리 적법성 근거 추가 등	<ul style="list-style-type: none"> <li>인정된 정당한 이익 목적을 처리 적법성 근거로 추가</li> <li>기타 정당한 이익 목적에 해당하는 처리의 예시 나열</li> </ul>	<ul style="list-style-type: none"> <li>제6조제1항 제(ea)호</li> <li>제6조제11항</li> </ul>
목적 제한 원칙 완화	<ul style="list-style-type: none"> <li>컨트롤러의 목적 내 개인정보 처리 제한을 완화, 새로운 처리 목적이 기존 처리 목적과 호환될 경우 개인정보 처리를 허용하고자 하는 취지</li> <li>컨트롤러가 용이하게 목적의 상호 호환성을 판단할 수 있도록 기준 및 방법 제시</li> </ul>	<ul style="list-style-type: none"> <li>제8A조</li> </ul>
특수 범주 개인정보 관련 추가 권한	<ul style="list-style-type: none"> <li>과학혁신기술부 장관은 하위규정 제정을 통해 UK GDPR 제9조의 특수 범주 개인정보 이외에 새로운 특수 범주 개인정보를 추가할 수 있음</li> </ul>	<ul style="list-style-type: none"> <li>제11A조</li> </ul>
접근권 행사 시 컨트롤러의 대응	<ul style="list-style-type: none"> <li>정보주체가 접근권 행사 시 컨트롤러가 추가 정보 제공을 요청할 수 있도록 함</li> <li>컨트롤러가 접근권에 대응하여 정보를 제공할 때 정보 검색 노력 정도 및 응답 기한 등을 명시</li> </ul>	<ul style="list-style-type: none"> <li>제12조</li> <li>제12A조</li> <li>제15조</li> </ul>
자동화된 의사결정 사용 제약 완화	<ul style="list-style-type: none"> <li>자동화된 의사결정 수단 활용을 장려하기 위해 해당 수단 사용 전 개인정보 처리의 적법성을 갖추도록 한 요건을 대폭 완화</li> </ul>	<ul style="list-style-type: none"> <li>제22조</li> </ul>
개인정보보호 테스트 제도 도입	<ul style="list-style-type: none"> <li>개인정보 국외이전 시 제3국의 적정성 평가 방식을, 개인정보보호 테스트 제도라는 보다 완화된 방식으로 대체</li> </ul>	<ul style="list-style-type: none"> <li>제45조</li> </ul>

출처: 법률안 분석을 통한 넥스텔리전스(주) 재구성

## (2) DPA 2018 개정

### 1) ICO 개편

■ 법안은 DPA 2018 제114A조를 신설하여 기존 영국 개인정보 감독기관(Information Commissioner's Office (이하 ICO))을 정보위원회(Information Commission)로 개편

- 기존 ICO는 커미셔너 단독 소유 형태(corporation sole)였으나 신설 정보위원회는 CEO 및



임원 등으로 이사회를 갖춘 법인체 형태(body corporate)로 변경됨

- 정보위원회는 또한 동법 신설조항인 제148A~148C조 및 기존 제142조, 제146조 개정 등에 따라 추가적인 정보 수집 및 조사 권한을 보유함으로써 조직의 개인정보 침해 시 해당 조직에 대한 강력한 집행권한을 행사
  - 구체적으로, 컨트롤러 등에 정보 및 문서 제공, 보고서 준비 등을 요구할 수 있으며, 컨트롤러의 임직원에게 면접 통지서를 발행함으로써 해당 임직원이 면접에 참석하여 질문에 답변하도록 요구하는 것이 가능
  - 만약 면접 중 해당 임직원이 질문에 대한 응답 과정에서 중요한 사항에 대해 허위임을 알면서 진술하거나 또는 무모하게(recklessly) 진술을 할 경우 법률 위반행위로 간주

## 2) 민원 제기 메커니즘 변경

**법안은 정보위원회에 접수되는 민원 관련 업무 부담을 완화하기 위해 DPA 2018 제164A조를 신설하여 정보주체가 정보위원회 대신 컨트롤러에 직접 민원을 제기하도록 하는 등 민원 제기 메커니즘을 변경**

- 정보주체는 자신과 관련된 개인정보와 관련하여 UK GDPR 위반 또는 DPA 2018 제3부 위반이 있다고 판단하는 경우 컨트롤러에 민원을 제기할 수 있음
- 컨트롤러는 전자적 또는 기타 방법의 민원 제기 양식을 제공하여 민원 제기가 용이하게 이루어지도록 지원해야 하며, 민원이 접수된 날로부터 30일 이내에 민원을 접수했음을 인정해야 함
- 민원을 접수한 컨트롤러는 지체 없이 민원에 대응하기 위한 적절한 조치를 취하고 그 처리 결과를 정보주체에게 알려야 함
  - 이때의 적절한 조치라 함은 민원사항에 대해 적절한 범위 내에서 문의하고 그 진행 상황을 정보주체에게 알리는 것이 포함됨

## (3) PECR 2003 개정

### 1) 쿠키 수집 관련 동의 요건 완화

**법안은 쿠키 수집 시 기존 PECR 2003의 '엄격히 필요한' 경우에 한정된 동의 면제 요건을 보다 완화하는 부칙(Schedule) A1을 신설**

- 단말기 접근과 관련하여 가입자 또는 이용자의 필수 동의 획득 요건을 담은 PECR 2003 제6조제1항은 다음의 경우 적용되지 않음
  - 전자 통신 네트워크를 통한 통신 전송을 수행하기 위한 목적으로, 가입자 또는 이용자의 단말기에 정보를 기술적으로 저장하거나 그러한 장비 내 저장된 정보에 기술적으로 접근하는 행위
  - 가입자 또는 이용자가 요청한 정보사회 서비스 제공을 위해 저장 또는 접근이 반드시 필요한 경우에 있어서, 가입자 또는 이용자의 단말기에 정보를 기술적으로 저장하거나 그러한 장비 내 저장된 정보에 기술적으로 접근하는 행위
  - 서비스 개선을 위한 서비스 이용 방식 등에 대해 통계 목적으로 정보를 수집하기 위해 정보사회 서비스 제공자가 가입자 또는 이용자의 단말기에 정보를 저장하거나 그러한 장비 내 저장된 정보에 접근하는 행위
  - 단말기가 특정 웹사이트에 접속할 때 작동하는 방식이 가입자 또는 이용자의 선호도에 맞게 조정되도록 하거나 특정 웹사이트 접속 시 웹사이트 모양이나 기능을 향상시킬 수 있도록 하기 위해, 정보사회 서비스 제공자가 가입자 또는 이용자의 단말기에 정보를 저장하거나 그러한 장비 내 저장된 정보에 접근하는 행위 등
- 위와 같이 동의 면제 요건을 대폭 완화함으로써 결과적으로 영국 온라인 이용자의 쿠키 수집 관련 팝업 빈도가 일정 부분 감소될 수 있음

## 2) 과징금 상황

### Ⅰ 법안은 PECR 2003의 집행을 강화하기 위해 기존 PECR 2003의 부칙1을 신설 부칙1로 대체함으로써 과징금 상한을 대폭 확대

- 전자통신 개인정보보호 위반 시 현행 최대 50만 파운드(약 9억원)의 과징금을 UK GDPR 및 DPA 2018 수준으로 대폭 상향
  - 즉, 기업의 경우 최대 1,750만 파운드(약 320억원) 또는 직전 회계연도 전 세계 연간 총 매출액의 4% 중 더 높은 금액에 해당하는 과징금 부과 가능

## (4) 기타 제도 개선

### Ⅰ 법안은 개인정보보호뿐만 아니라 데이터 활용 측면에서도 여러 개선사항을 도입

- (보건 데이터 표준 확립) 보건 분야의 IT 시스템은 플랫폼 간 데이터 공유를 가능케 하기 위해 공통의

정보 표준을 충족해야 함 (2012년 건강 및 사회복지법(Health and Social Care Act 2012) 개정)

- 정보 표준에는 기능, 연결성, 상호 운용성, 이동성, 정보 저장 및 접근, 정보 보안에 관한 항목을 포함하여 정보 기술 또는 IT 서비스에 관한 기술적 사항이 포함될 수 있음
- **(데이터 접근성 강화(일명 스마트 데이터))** 각부장관은 데이터 보유자(data holder)에 해당하는 상품 및 서비스 공급자가 우월적 시장 지위를 이용하여 고객 데이터를 독점하지 못하도록 하위규정을 제정함으로써 공급자 간 경쟁을 촉진할 수 있음 (데이터(이용 및 접근) 법(안) 제1부 신규 제정)
  - 각부장관은 하위규정을 제정하여 데이터 보유자로 하여금 고객의 요청에 따라 고객 및 비즈니스 데이터를 고객에게 직접 제공하거나, 고객이 데이터를 수신하도록 권한을 부여한 자에게 제공하도록 할 수 있음
  - 또한 하위규정에서 데이터 보유자가 고객 데이터를 생성, 수집 또는 보관하고, 부정확한 데이터를 수정하는 등 고객 데이터를 변경하도록 규정할 수 있음
  - 그밖에, 하위규정을 통해 데이터 보유자로 하여금 대시보드 서비스, 전자통신 서비스 또는 애플리케이션 프로그래밍 인터페이스를 등 지정된 시설이나 서비스를 활용하여 데이터 접근 및 이용을 가능케 하도록 할 수 있음
- **(디지털 검증 서비스 제도 도입)** 정부는 특정 요건을 충족한 디지털 신원 검증 서비스 제공자에 정부에서 인증한 신뢰 마크(trust mark)를 부여하는 제도를 도입하여, 해당 신원 검증 서비스에 대한 데이터 보호의 신뢰성 및 시민의 일상 생활의 다양한 측면에서 효율성을 높이고자 함 (데이터(이용 및 접근) 법(안) 제2부 신규 제정)
  - 각부장관은 디지털 검증 서비스 등록부를 설치 및 유지·관리하여 디지털 검증 서비스를 제공하는 조직 목록을 제공하고 이를 공개적으로 열람할 수 있도록 함
  - 디지털 검증 서비스 제공 조직은 해당 등록부에 등재되기 위해 공인된 적합성 평가 기관에서 발급한 인증서를 보유하는 등 특정 기준을 충족해야 함
  - 각부장관은 디지털 검증 서비스 등록부에 등재된 조직만 사용할 수 있는 신뢰 마크<sup>2)</sup>를 지정할 수 있는 권한을 가짐

2) 조직은 신뢰 마크를 통해 ▲제3자 마케팅 목적으로 이용자 프로파일링을 수행하지 않음 ▲이용자의 민감 데이터가 공개될 위험이 있는 대규모 데이터 세트를 생성하지 않음 ▲이용자가 자신의 개인정보가 어떻게 공유되고 있는지 충분히 인지하고 있음 등 높은 수준의 표준을 충족하고 있음을 나타낼 수 있음

### 3. 기타 사항

■ 법안은 급진적인 데이터 제도 개혁에 대한 논란을 피하고 EU집행위원회의 영국에 대한 적정성 지위를 안전하게 유지시키기 위해 쟁점이 되었던 일부 개인정보보호 개혁 조치를 제외

**표 2** 데이터(사용 및 접근) 법(안)에서 제외된 개인정보보호 관련 개정 사항

구분	내용	비판점	비고
개인정보에 대한 정의 변경	<ul style="list-style-type: none"> <li>개인정보 정의를 합리적인 수단을 통해 컨트롤러 또는 제3자가 식별할 수 있는 정보로 제한</li> </ul>	<ul style="list-style-type: none"> <li>법률 적용범위를 실제로 좁히는 것인지, 아니면 단순히 명확성을 높이는 것인지에 대한 논란 제기</li> </ul>	<ul style="list-style-type: none"> <li>불포함</li> </ul>
접근권 행사에 대한 컨트롤러의 거부 권한	<ul style="list-style-type: none"> <li>정보주체의 개인정보 접근권 행사 시 접근 요청을 거부하거나 접근권에 대한 비용 청구를 가능하게 하는 기준을 '명백히 근거가 없거나 (manifestly unfounded) 과도함'에서 '성가 시거나(vexatious) 과도함'으로 완화</li> </ul>	<ul style="list-style-type: none"> <li>영국의 기타 관련 법률과의 일관성을 위한 개선사항이었으나 추가적인 불명확성을 초래한다는 비판</li> </ul>	<ul style="list-style-type: none"> <li>불포함</li> </ul>
처리 활동 기록 의무	<ul style="list-style-type: none"> <li>컨트롤러의 처리 활동 기록 의무 요건을 좁혀 개인에게 높은 위험을 초래할 가능성이 있는 처리(고위험 처리)에만 적용</li> </ul>	<ul style="list-style-type: none"> <li>일련의 컨트롤러 의무와 관련해, 각 조직의 의무 준수부담을 줄이고자 하는 시도였으나, 제도 개혁에 관한 이익 대비 실효성 측면에서 의문이 제기</li> </ul>	<ul style="list-style-type: none"> <li>불포함</li> </ul>
DPO 지정 의무	<ul style="list-style-type: none"> <li>DPO를 폐지하고 이를 고위 책임자(senior responsible individuals)로 대체               <ul style="list-style-type: none"> <li>- DPO 대신 조직 내 고위급 임원이 DPO 역할을 수행하도록 하여 조직의 부가적인 의무사항을 완화하려는 취지</li> </ul> </li> </ul>		
개인정보 영향평가 수행 의무	<ul style="list-style-type: none"> <li>처리 유형이 개인의 권리와 자유에 중대한 위험을 초래할 때 수행해야 하는 개인정보 영향 평가를 고위험 처리 평가(assessments of high-risk processing)로 대체</li> </ul>		
국내대표자 임명 의무	<ul style="list-style-type: none"> <li>영국 외부의 기업/조직이 영국 내 개인정보를 다룰 경우 국내대표자를 임명해야 한다는 의무사항을 제거</li> </ul>		

출처: 법률안 상호 비교를 통한 넥스텔리전스(주) 재구성

## 출처 |

1. Clifford Chance, How does the Data (Use and Access) Bill compare to its predecessor?, 2024.11.04.
2. DLA Piper, UK: Data (Use and Access) Bill: newcomer or a familiar face?, 2024.11.05.
3. EdwinCoe, The new UK Data (Use and Access) Bill – what you need to know, 2024.11.07.
4. Hunton Andrews Kurth, What's New in the Draft UK Data (Use and Access) Bill?, 2024.11.21.
5. Infosecurity Magazine, UK Government Introduces New Data Governance Legislation, 2024.10.24.
6. Osborne Clarke, The UK Data (Use and Access) Bill – what businesses should be aware of, 2024.10.28.
7. Reynolds Porter Chamberlain, New Data (Use and Access) Bill, 2024.11.26
8. Slaughter and May, UK data reform presses ahead: Data (Use and Access) Bill introduced to UK Parliament, 2024.10.30.
9. Taylor Wessing, What's changing and what's the same in the UK's Data (Use and Access) Bill from a GDPR compliance perspective?, 2024.11.19.
10. Travers Smith, The Data (Use and Access) Bill – limited data protection reforms in the pipeline, 2024.11.07.



# 영국 ICO, CMA, 온라인 선택 아키텍처의 유해한 설계 사례와 개인정보 악영향 고찰

## [목 차]

### 1. 온라인 선택 아키텍처(OCA)의 중요성과 영향력

- (1) OCA의 중요성 및 영향력
- (2) ICO와 CMA가 OCA를 주목하는 배경
- (3) 보고서의 목적

### 2. 온라인 선택 아키텍처(OCA)의 악영향과 피해

- (1) 데이터 보호 측면의 피해
- (2) 개인정보 처리와 관련된 경쟁 및 소비자 보호 피해

### 3. 잠재적으로 유해한 OCA 관행 사례

- (1) 유해한 넛지 및 슬러지(Harmful nudges and sludge)
- (2) 컨펌셰이밍(Confirmshaming)
- (3) 편향된 프레이밍(Biased framing)
- (4) 번들된 동의(Bundled consent)
- (5) 디폴트 설정(Default setting)

### 4. 올바른 OCA 관행 정착을 위한 방안

## 1. 온라인 선택 아키텍처(OCA)의 중요성과 영향력

### (1) OCA의 중요성 및 영향력

■ '24년 11월 4일, 영국 개인정보 감독기관 ICO(Information Commissioner's Office)와 시장 경쟁 감독기관 CMA(Competition and Markets Authority)는 디지털 시장에서 온라인 선택 아키텍처(OCA) 관행이 개인정보보호와 시장 경쟁에 미치는 악영향을 고찰한 공동 보고서를 발표

- 온라인 선택 아키텍처(OCA)는 디지털 시장에서 기업이 웹사이트 및 기타 온라인 서비스 사용자에게 정보와 선택권을 제공하는 방식을 의미
- OCA 관행(practice)은 가격의 표시 방식, 구매 상품과 서비스에 대한 정보가 소비자에게 제공되는 방식 등 디지털 시장 전반의 광범위한 행동들을 포괄
- ICO와 CMA는 OCA가 개인정보를 수집, 추가 처리, 공유 방식에 대한 사용자의 결정과

행동에 영향을 미치고 있으며, 사용자가 자신의 정보와 개인정보 보호권을 행사하는 방식에도 영향을 준다고 분석

- 양 기관은 OCA 관행이 맞춤형 추천 같은 개인화된 서비스 제공이 보편화된 디지털 시장에서 사용자 경험에 영향을 미치고, 궁극적으로는 제품·서비스를 제공하기 위해 개인정보 접근에 의존하는 기업 경쟁 결과에도 영향을 미친다고 인식
- (긍정적 영향) 잘 설계된 OCA는 사용자가 자신의 목표, 선호도, 최선의 이익에 부합하는 선택을 하도록 유도
  - 가령, 기본적인 보안 설정을 모든 사용자에게 적용함으로써, 바이러스 대한 대응력과 사이버보안 역량을 강화
  - 또한 효과적인 OCA는 사용자에게 개인정보 수집 및 사용 방식에 대한 올바른 선택을 지원하며, 기업의 광고 타겟팅에 동의 여부를 선택할 수 있는 다양한 선택권 제공
  - 빠르고 원활한 반품 절차 등과 같이 웹사이트 인터페이스를 보다 직관적이고 쉽게 설계하여 사용자 경험 개선과 함께 기업의 공정 경쟁을 위한 인센티브를 강화
- (부정적 영향) 반면, OCA 관행은 개인의 개인정보 통제권을 약화시키고 사용자가 개인정보 사용에 대한 이익이나 선호에 부합하지 않는 유해한 행동을 하도록 유도할 가능성도 존재
  - 유해한 OCA 관행은 사용자가 특정 결정을 내리도록 설계된 인터페이스나 선택권을 부당하게 제한함으로써, 개인정보 보호권, 소비자 권리, 시장 경쟁에 악영향

## (2) ICO와 CMA가 OCA를 주목하는 배경

### Ⅰ OCA 관행은 디지털 시장에서 사용자의 데이터가 수집, 사용, 공유되는 방식으로, 이는 소비자 정보와 개인정보 보호권에 영향을 미치기 때문에 ICO가 주목

- ICO는 '22년 11월 'ICO25 전략(ICO25 Strategic Plan)'을 통해 디지털화가 가속화되는 환경에서 사용자가 온라인 공간에서 개인정보에 대한 의미 있는 통제(meaningful control)와 신뢰를 확보할 수 있도록 하겠다고 공언
  - 구체적으로 ICO는 개인정보 처리가 포함된 온라인 선택 구조 설계 과정에서, 더 높은 수준의 표준 마련과 적용을 추진
  - 이를 통해 대중이 디지털 시장에서 자신의 데이터가 어떻게 사용되는지 확신을 갖고, 개인정보 및 개인정보 보호권이 침해된 우려 없이 혁신적인 제품과 서비스 혜택을 누릴 수 있도록 지원하겠다는 것이 목표

## Ⅰ CMA는 OCA가 기업의 경쟁 방식과 소비자 대우 방식에 미치는 영향 때문에 관심 보유

- CMA는 OCA 관행 전반에 걸쳐 지속적이고 적극적으로 관련 프로그램을 운영
  - CMA는 '22년 디지털 디자인이 경쟁과 소비자에게 미칠 수 있는 부정적 영향에 대한 토론 보고서를 발표
  - 또한 소비자 교육과 관련 조치를 이행하면서, 유해한 OCA 관행에 대응해 왔으며, 유해한 온라인 판매 관행에 대처하는 광범위한 작업 프로그램을 시작

### (3) 보고서의 목적

## Ⅰ OCA 관행이 잘못 설계되거나 오용될 경우 발생할 수 있는 피해와 구체적 사례를 소개하는 것이 보고서의 1차적인 목적

- 개인정보 처리와 관련된 유해성 있는 OCA 관행에 관해 설명하고, 이러한 관행이 CMA와 ICO에 공통된 우려를 불러일으킨 이유를 설명
  - ICO와 CMA는 유해성 있는 OCA 관행의 사례를 ①유해한 넛지·슬러지(Harmful nudges and sludge), ②컨펌셰이밍(Confirmshaming), ③편향된 프레이밍(Biased framing), ④번들된 동의(Bundled consent), ⑤디폴트 설정(Default setting)으로 제시
- 예시를 통해 기업들이 개인정보 처리 시 우려되는 OCA 관행에 대해 보다 명확히 이해할 수 있도록 하고, 온라인 서비스를 접속 및 사용하는 소비자는 개인정보보호 강화 및 시장 경쟁 촉진을 위한 다양한 OCA가 어떻게 사용될 수 있는지에 대한 지침을 제공

## Ⅰ ICO와 CMA가 제시하는 기대치를 충족하지 못하고, 소비자에게 피해를 줄 가능성이 있는 기업에 대해 아래와 같은 양 기관이 취할 수 있는 규제 조치를 경고하는 것도 본 보고서의 목적

- (ICO 규제 방식) 데이터 보호법을 준수하지 않는 경우, 사람들을 보호하고 피해를 방지하기 위해 필요에 따라 공식적인 집행 조치를 사용할 수 있음을 명시
- (CMA 규제 방식) 경쟁하는 기업과 소비자를 보호하는 프레임워크를 구축하고, 이러한 목표를 달성하기 위해 필요한 경우 집행 조치를 이행

## 2. 온라인 선택 아키텍처(OCA)의 악영향과 피해

### (1) 데이터 보호 측면의 피해



**Ⅰ 영국 데이터보호법은 개인정보를 처리하는 기업이 데이터 활용에 대한 책임을 지도록 규정하고 있으며, 위험 기반 접근 방식을 채택하고 있으며, 기업은 데이터 처리로 인한 잠재적 피해를 고려해야 하지만, 잘못된 OCA 관행은 아래와 같이 데이터 보호법에 위배될 수 있음**

- (부당한 침입 초래) 잘못된 OCA 관행은 디지털 서비스 사용자가 본인의 선호에 맞지 않는 개인정보를 선택하도록 조작하고 영향을 미칠 가능성 존재
  - 예를 들어, 자발적으로 동의한 것보다 더 많은 개인정보를 공유하게 하여, 이를 통해 행동, 선호도 및 태도 관련 광범위한 개인정보가 확보되면서, 궁극적으로 원치 않는 타겟 광고 또는 프로파일링과 같은 부당한 소비자 침해가 초래
- (통제권 및 자율성 상실) 잘못된 OCA 관행은 사용자가 자신의 데이터 처리 방식을 자유롭게 선택하는 것을 어렵게 만들고 개인정보가 사용되는 방식에 대한 의미 있는 통제권을 박탈
- (피해 방지 또는 완화 비용 발생) 잘못된 OCA 관행으로 개인정보 처리와 관련해 정보에 입각한 선택을 하거나 개인정보보호 기본 설정에 부합하는 조치를 취하는데 시간·비용이 소모
- (개인 기본권과 자유에 악영향) 자유로운 선택권을 훼손하고 낮은 수준의 프라이버시를 정상 상태로 간주하는 잘못된 OCA 관행이 확산되면 개인의 기본권과 자유에도 악영향

## (2) 개인정보 처리와 관련된 경쟁 및 소비자 보호 피해

**Ⅰ OCA를 활용하여 소비자가 원하는 것보다 더 많은 개인정보를 수집하거나, 자사 서비스에 대한 데이터 수집을 강화함으로써 시장 지위를 강화하여 경쟁을 약화시키는 방식으로 소비자 피해 발생**

- OCA를 활용하여 경쟁사 대비 더 많은 소비자 데이터를 수집한 기업은 아래와 같은 방식으로 시장 입지를 강화하거나 경쟁을 약화시킬 가능성 존재
  - 제품이나 서비스의 장점이거나 경쟁력에 기반하지 않고도 시장 입지 강화 가능
  - 소비자가 현재 공급자로부터 전환하기 어렵게 만드는 종속성 생성
  - 경쟁사가 경쟁을 하기 어렵게 만들어, 시장 진입 및 확장 장벽을 조성하는 등 경쟁 약화
- OCA는 특정 옵션을 다른 옵션보다 선택하기 더 쉽게 만들거나, 더 바람직하게 보이도록 함으로써, 아래와 같은 소비자 선택을 왜곡하는 데 악용될 소지
  - 독립적으로 정보를 처리하고 평가하는 능력을 약화시키거나 쇼핑을 더 어렵게 만들어, 소비자의 신중한 선택을 방해(ex. 정보 처리 및 평가 능력을 약화)
  - 소비자에게 선택 사항을 불명확하게 표현
  - 소비자가 잠재적으로 바람직하지 않은 서비스 또는 행동에 동의하도록 유도함으로써, 소비자 후생을 감소시키고, 소비자 선호에 부합하지 않을 수 있는 신중하지 못하거나 부주의한 결정을 하도록 유도

### 3. 잠재적으로 유해할 수 있는 OCA 관행 사례

#### (1) 유해한 넋지 및 슬러지(Harmful nudges and sludge)

■ 유해한 넋지는 사용자가 부주의하거나 신중하지 못한 결정을 내리도록 특정 선택을 유도하는 설계를 의미하며, 유해한 슬러지는 사용자가 원하는 선택을 하기 어렵게 만드는 과도하거나 부당한 마찰(슬러지)을 유발함으로써 소비자 선택을 왜곡

- 유해한 넋지 및 슬러지는 기업이 한 옵션을 다른 옵션보다 훨씬 덜 번거롭거나 시간이 덜 걸리게 하여, 특정 옵션을 다른 옵션보다 선택하도록 유도하여 소비자의 선택을 왜곡
- 이 OCA 관행이 사용될 경우, 소비자는 다른 방법으로는 하지 않았을 선택을 하거나 자기 최선의 이익이나 선호도에 부합하지 않는 선택을 하게 될 가능성이 높아짐
  - 가령, 소비자가 개인정보를 설정할 경우에, 프라이버시를 덜 강화하는 선택을 하게 하거나 개인정보 설정 변경을 어렵게 만드는 것이 사례

■ (사례) 서비스의 개인화 수준 설정 과정에서, 사용자는 한 단계로 모든 개인화 기능을 설정할 수 있으나, 개인화를 끄려면 여러 단계를 거쳐야 하며, 모든 개인화를 한 번에 거부할 수 있는 옵션이 없는 경우

- 이 경우, 사용자는 모든 개인 맞춤화를 수락하도록 유도되는 반면, 회사는 개인 맞춤화를 통해 개인정보를 더 세밀하게 제어하거나 개인 맞춤화를 완전히 거부하는 것을 방해
- (ICO의 우려) 사용자가 콘텐츠에 빠르게 접근하거나, 자세하게 설정할 시간이나 지식이 없는 상황에서, 사용자가 자신의 결정에 대해 숙고하지 못하게 함으로써 아래와 같은 위법 발생 우려
  - 이러한 방식으로 수집된 개인정보 처리 동의는 정보 제공이 이루어지지 않을 가능성이 높으므로 영국 일반데이터보호규정(UK General Data Protection Regulation, GDPR) 5조 1(a)항 '공정성' 및 '투명성' 원칙을 침해할 우려
  - 쿠키 배치에 대한 동의를 유도하는 쿠키 배너를 사용하는 경우, '개인정보보호 및 전자 통신 규정 2003 (Privacy and Electronic Communications Regulations(PECR) 2003)' 6조 침해 우려
- (CMA의 우려) 유해한 넋지와 슬러지가 사용자로 하여금 해당 서비스를 이용하기 위해 더 많은 개인정보를 제공하도록 유도
  - CMA 온라인 플랫폼 및 디지털 광고 시장 연구 최종 보고서에서는 이러한 개인정보에 대한 접근이 특정 대형 플랫폼에 경쟁 우위를 부여하고 중소기업의 진입과 확장을 저해한다고 분석
- 다만, 모든 넋지와 슬러지가 유해한 것은 아니며 책임감 있게 구현할 경우 사용자 이익에 부합하는 것도 가능
  - 예를 들어, 넋지는 사용자가 원할 경우, 다른 은행 계좌로 쉽게 전환되도록 하는 등 사용자에게 이익이 되는 결정을 유도하는 데 활용 가능

- 슬러지의 경우에도, 사용자에게 다른 은행 계좌로 거액을 이체하기 전에 확인 요청 등 중요한 결정을 재확인하거나 검증하는데 활용된다면 소비자의 이익을 위한 결정 유도

## (2) 컴펄세이밍(Confirmshaming)

### Ⅰ 컴펄세이밍은 특정 행동을 하지 않을 경우 죄책감이나 수치심을 느끼게 함으로써 특정 행동을 하도록 압박하는 OCA 설계 구조를 의미

- ‘좋은’ 선택과 ‘나쁜’ 선택이 있음을 명확히 암시하는 언어를 사용하거나, 더 극단적인 경우에는 특정 행동을 하지 않는 것이 도덕적으로 잘못되었거나 사회적으로 용인될 수 없다는 식의 표현을 사용
- 컴펄세이밍 관행은 사용자가 다른 방법으로는 동의하지 않을 개인정보 사용에 동의하게 함으로써, 궁극적으로 사용자의 선택에 부정적 영향을 미침
  - 일부 관련 연구에 의하면, 디지털 시장에서 웹사이트 사용자들은 서비스를 거부할 수 있는 옵션이 수치스러운 것으로 묘사될 때, 의심스러운 서비스를 받아들이 가능성이 더 높은 것으로 분석
  - 따라서, 컴펄세이밍 관행을 사용할 경우, 죄책감이나 당혹감을 특정 선택과 다른 선택과 연관시켜 사용자의 선택을 왜곡시킬 우려 존재

### Ⅱ (예시) 사용자에게 할인을 받는 대가로 이메일 주소를 제공하도록 요청하는 팝업에 대해서 사용자가 요청을 거부하기 위해서는 ‘아니요 할인은 싫어요’라는 버튼을 클릭해야 하는 경우가 해당

- (ICO의 우려) 개인정보 제공 동의를 거부하는 사용자에게 부정적이거나 압박하는 문구를 적용하는 것은 영국 GDPR의 주요 원칙에 위배배
  - 사용자를 압박하는 문구를 활용하여 받아낸 동의는 영국 GDPR 제5조 1(a)항의 ‘공정성’ 원칙을 침해할 가능성이 높고, 이 같은 동의는 자유롭게 제공된 것으로 보기 어려우므로 제4조 11항에 따라 무효가 될 가능성이 높을 뿐만 아니라, 제5조 1(a)항의 ‘적법성’ 원칙에도 위배
- (CMA의 우려) 컴펄세이밍 관행은 사용자가 보다 많은 개인정보를 공유하도록 유도할 수 있는 만큼, 특정 시장에서는 이러한 데이터에 대한 접근이 기존 사업자에게 경쟁 우위를 부여하고 소규모 도전 기업의 진입을 억제할 우려 존재

## (3) 편향된 프레임링(Biased framing)

### Ⅰ 편향된 프레임링이란 특정 옵션의 예상되는 혜택이나 긍정적인 결과를 강조하거나, 반대로 위험이나 부정적인 결과를 강조하여 사용자가 해당 옵션을 선택하지 못하도록 하는 관행을 의미

- 긍정적 프레임 또는 부정적 프레임 기법을 오용하면 사용자가 잘못된 정보를 바탕으로 잘못된 선택을 하게 되고, 더 유리한 프레임을 선택하는 방향(또는 불리한 프레임의 선택에서 멀어지게 하는 방향)을

유도하여 의사 결정을 왜곡

- 디지털 시장에서는 타겟 광고나 예상치 못한 마케팅에 사용될 개인정보가 원치 않게 수집될 수 있으며, 이에 따라 개인에게 잠재적인 피해 위험이 증가할 가능성 존재

**I (예시) 특정 기업에서 검색 기록 공유 의향을 물어보면서 검색 기록을 공유하면, 서비스를 맞춤화하여 필요한 정보를 정확하게 제공할 수 있고, 표시되는 광고 관련성도 높아지지만, 검색 기록을 공유하지 않을 것 경우, 정보 및 광고가 관련성이 떨어지거나 유용하지 않을 수 있다고 설명하는 경우**

- (ICO의 우려) 개인 데이터 처리에 대한 결정의 위험과 이점에 동일한 가중치를 부여하지 않을 경우, 사용자가 정보를 제대로 평가하고 정보에 입각한 선택을 하기 어렵기 때문에, 영국 GDPR 제5조 1(a)항의 공정성, 투명성 원칙에 위배됨. 또한 편향된 프레임을 통해 얻은 동의는 충분한 정보를 제공하지 않은 동의이기 때문에 영국 GDPR 7조의 적법성 요건에도 위배
- (CMA의 우려) 기존 시장 진입 기업들이 편향된 프레이밍 관행을 활용하여 개인정보 수집 및 경쟁 우위를 확보하고, 소규모 경쟁 업체의 진입·확장을 억제하거나, 소비자들이 경쟁사보다 자사 서비스를 선호하도록 하는데 편향된 프레이밍을 악용

#### **(4) 번들된 동의(Bundled consent)**

**I 번들된 동의는 사용자에게 한 번에 여러 개의 개별 목적이나 처리에 대한 개인정보 사용 동의를 요청하는 것을 의미하며, 사용자가 개인정보에 대한 세분된 통제권을 행사하기 더 어렵게 함**

- 일괄 동의는 사용자가 원하는 기능에 접근하기 위해 타겟 광고나 다이렉트 마케팅 등 원하지 않는 개인정보 처리에 의도치 않게 또는 실수로 동의하는 잘못된 결정을 내리는 결과 초래
- 사용자가 원할 경우 계정 설정에서 관련 옵션을 찾아 세분된 통제권을 행사할 수 있지만, '모두 동의' 옵션을 제공하면 실제 사용자 선호도와 맞지 않더라도 모든 처리에 동의할 가능성 존재

**I (예시) 계정 가입 절차의 일부로 서비스 개인화에 필요한 개인정보 처리와 계정 개인화와 직접 관련이 없는 쿠키 설정에 대한 일괄 동의를 요청할 경우**

- 사용자는 해당 회사가 제공하는 모든 서비스의 개인화 및 쿠키 설정에 동의하거나, 모든 서비스에 대한 동의를 거부해야 하며, 나중에 개별 동의를 변경할 수 있으나, 결과적으로 사용자가 모든 처리 활동에 동의할 가능성을 높이고, 나중에 동의를 철회할 가능성을 줄이고자 시도
- (ICO의 우려) 영국 GDPR 제4조 11항에서 개인 데이터 처리에 대한 동의는 '구체적'이어야 하며, 제7조 4항은 필요한 경우가 아니라면 동의를 서비스 조건으로 묶어서는 안 된다고 명시
- 번들된 동의는 구체성이 낮고, 충분한 정보가 제공이 이루어지지 않을 수 있어, 세분된 동의 옵션보다 무효가 될 가능성이 있음. 또한 및 5조 1(a)항의 적법성 요건을 위반할 가능성도 존재

- (CMA의 우려) 특정 기업이 번들된 동의 관행을 사용하여 모든 자사 서비스에서 데이터 공유에 대한 동의를 한데 묶어 사용자 데이터를 더 많이 수집할 경우, 경쟁에 대한 우려가 발생

## (5) 디폴트 설정(Default settings)

### I 기업은 '디폴트 설정'을 통해 사용자가 적극적인 조치를 취하지 않을 경우 자동으로 사전 정의된 선택 사항을 적용하는데, 이는 사용자의 효과적인 선택 능력을 저하시킬 우려 존재

- 사용자가 기본 설정을 변경하려면 설정 사항을 자세히 살펴보게 하거나, 정기적 구독을 취소하고자 할 경우, 전화 등 다른 방법으로 연락하게 함으로써, 기본 설정을 변경하지 못하도록 유도할 수 있으며, 아래와 같은 이유로 소비자의 능동적 선택을 저해
  - 사용자가 바쁘거나 관심이 없거나 다른 요소에 더 집중하는 경우, 디폴트 설정을 변경하기보다 그대로 유지할 가능성이 더 높음
  - 디폴트 설정값이 회사의 보증 또는 추천이거나 대부분 사용자가 선택한 옵션으로 인식할 소지
  - 디폴트 설정값은 사용자가 기본 옵션을 이미 선택한 것처럼 행동하도록 유도하며, 사용자들은 결과적으로 디폴트 설정값을 기준으로 삼아 선호도를 구성

### I (예시) 소셜네트워크에서 게시하는 콘텐츠 공개 범위가 기본적으로 모든 사람이 볼 수 있게 디폴트 설정이 되어 있는 가운데, 비공개로 설정하려면 계정 설정으로 이동하여 별도 설정 작업이 필요한 경우

- (ICO의 우려) 영국 GDPR 25조에서는 기업에게 기본값 해제 방식을 채택할 것을 요구하지는 않지만, 처리 상황과 개인에게 제기되는 위험을 고려해야 한다고 규정하고 있으며, 기업들은 기본적으로 개인 데이터가 불특정 다수의 자연인에게 접근되지 않도록 해야 한다고 규정
  - 25조를 준수하지 않으면, 5조 제1항(a)의 '공정성' 원칙 및 제5조 제1항(c)의 데이터 최소화 요건 등 다른 조항을 위반할 위험성도 존재
  - 또한 개인이 동의를 표시하려면 적극적인 조치를 취해야 하므로 기본 설정을 통해 얻은 동의는 GDPR 제5조 제1항(a)의 적법성 원칙을 위반할 수 있으며, 변경되지 않은 기본 설정을 비필수 쿠키 설정에 대한 동의로 간주하는 경우 PECR 제6조에 위배
- (CMA의 우려) 디폴트 설정으로 인해 사용자가 원하는 것보다 더 많은 데이터를 공유하거나 실수로 자동 갱신 구독 플랜에 등록하는 등 본인의 이익에 최선이 아닌 선택을 하게 될 소지가 있으며, 사용자가 다른 상품과 서비스를 둘러보거나 탐색하는 능력을 제한함으로써, 가장 활동성이 낮은 고객이나 가장 유용한 데이터를 먼저 확보한 기존 사업자에게 유리하게 작용

## 5. 올바른 OCA 관행 정착을 위한 방안

ICO-CMA 공동 보고서는 데이터 보호, 경쟁 및 소비자 보호 관점에서 OCA 관행의 유해성 위험 완화를 위해 기업들이 OCA 설계 시 아래 4대 질문을 고려해야 한다고 권고

**표 1** 올바른 OCA 관행 정착을 위한 권고안

권고안	질문 및 세부 설명
1. 사용자를 OCA 설계 선택의 중심에 두기	<ul style="list-style-type: none"> <li>• <b>(질문) 기업은 사용자의 관심사와 선호도를 중심으로 인터페이스를 구축하고 있나?</b> <ul style="list-style-type: none"> <li>- (과제) OCA 기본 설정은 사용자 관심을 반영하여 방식으로 설계되어야 하며, 기업이 사용자 프롬프트 디자인 및 사용자 데이터와 관련된 개입을 모색하고 있는 경우, 이러한 개입을 통해 사용자의 통제권과 개인정보보호 기본 설정을 행사할 수 있는 능력을 향상시킬 필요</li> </ul> </li> </ul>
2. 사용자 선택권/통제권 강화 디자인 사용	<ul style="list-style-type: none"> <li>• <b>(질문) 기업은 사용자가 자신의 개인정보에 대해 효과적이고 정보에 입각한 선택을 할 수 있도록 돕고 개인정보 수집 및 사용 방법을 사용자가 통제할 수 있도록 하고 있나? 정보가 명확하고 오해의 소지가 없나?</b> <ul style="list-style-type: none"> <li>- (과제) OCA는 어떤 개인정보가 수집되고 어떻게 사용되는지에 대해 이해하기 쉽고 균형 잡힌 정보를 제공하여 사용자가 자신의 개인정보 처리와 관련하여 제공 되는 약관에 동의할지 여부를 의미 있고 자유롭게 결정할 수 있도록 지원하는 방식으로 설계되어야 할 필요</li> </ul> </li> </ul>
3. 테스트 및 시험 설계 선택	<ul style="list-style-type: none"> <li>• <b>(질문) 기업은 OCA 설계가 근거에 기반하도록 테스트와 시험을 사용하나?</b> <ul style="list-style-type: none"> <li>- (과제) OCA 관행 설계는 소비자의 이해도, 경험 및 통제감뿐만 아니라 행동에 테스트로 가장 좋은 정보를 얻을 수 있으며, 이 같은 테스트는 소비자 피해가 어떻게 발생하는지 이해하고 잘못된 소비자 결과의 위험을 완화하는데 기여</li> </ul> </li> </ul>
4. 데이터 보호, 소비자 및 경쟁법 준수 여부	<ul style="list-style-type: none"> <li>• <b>(질문) 기업에서 채택하고 있는 OCA 관행이 데이터 보호, 소비자 보호 및 경쟁법에 미치는 영향을 고려했나?</b> <ul style="list-style-type: none"> <li>- (과제) 기업은 OCA 관행이 사용자에게 불공정하거나 반경쟁적(ex. 경쟁사 대비 부당한 이점을 제공하는 등)일 수 있음을 인지하고, 불공정 및 반경쟁적 가능성을 점검하고, 개인 데이터 처리와 관련된 OCA 관행이 항상 경쟁, 소비자 보호 및 데이터 보호 요건을 준수하도록 노력할 필요</li> </ul> </li> </ul>

### 출처 |

1. ICA-CMA, How Online Choice Architecture practices can undermine consumer choice and control over personal information, 2024.11.04.
2. DataGuidance, UK: ICO and CMA publish joint position paper on harmful design in digital markets, 2024.11.05.

# 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
17	9월 1호	X 플랫폼(구 트위터)의 Grok AI 챗봇 관련 GDPR 위반사례 분석
18	9월 2호	LLM 대안으로서의 LAM, 최신 동향과 개인정보보호 이슈
19	10월 1호	슈렘스 사건 등 CJEU의 최신 개인정보보호 관련 결정례 분석
20	10월 2호	호주 정부, 고위험 AI 안전장치 제안 협의 및 자발적 AI 안전 표준 발표
21	11월 1호	EU 법제상 AI 시스템 배포자의 DPIA 주요 검토사항
22	11월 2호	영국 데이터(사용 및 접근) 법(안) 주요 개정 사항 분석
23	11월 3호	영국 ICO, CMA, 온라인 선택 아키텍처의 유해한 설계 사례와 개인정보 악영향 고찰

# 2024 개인정보보호 월간동향분석

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

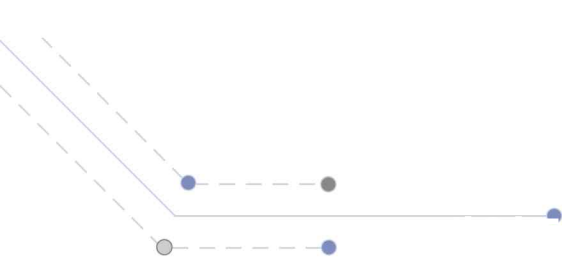
한국인터넷진흥원의 승인 없이 본 보고서의 무단전재나  
복제를 금하며, 인용하실 때는 반드시  
『2024 개인정보보호 월간동향 분석 보고서』라고  
밝혀주시기 바랍니다.

본 보고서의 내용은  
한국인터넷진흥원의 공식 견해가 아님을 알려드립니다.

## 발행

**발행일** 2024년 12월  
**발행처** 한국인터넷진흥원 개인정보제도팀  
전라남도 나주시 진흥길 9  
Tel : 061-820-1231





# 2024 개인정보보호 월간동향분석

2024 Vol.11

## PRiVACY REPORT

