

# PRiVACY REPORT

## 개인정보보호 월간동향분석

2024년 12월호



### | CONTENTS |

2024년 12월호

1

해외 주요 개인정보 감독기관 연례보고서

2

2024년 주요 개인정보보호 실태 서베이 보고서 분석

3

미국 연방거래위원회(FTC)의 개인정보보호 및  
정보보안 관련 집행 트렌드 분석



# 해외 주요 개인정보 감독기관 연례보고서

## [목 차]

1. 아일랜드 DPC(Data Protection Commission)
  - (1) 2023년 주요 활동 및 성과
  - (2) 정책/전략 및 주요 관심 영역
2. 영국 ICO(Information Commissioner's Office)
  - (1) 2023년 주요 활동 및 성과
  - (2) 정책/전략 및 주요 관심 영역
3. 프랑스 CNIL(Commission nationale de l'informatique et des libertés)
  - (1) 2023년 주요 활동 및 성과
  - (2) 정책/전략 및 주요 관심 영역

## 1. 아일랜드 DPC<sup>1)2)</sup>

### (1) 2023년 주요 활동 및 성과

■ DPC는 2023년에 개인으로부터 11,200건의 신규 민원을 접수했으며, 이는 2022년 대비 20% 증가한 수치

- 2023년에 접수된 민원 중 2,600건이 불만 처리 과정으로 진행되었으며, 이 중 8,600건이 비교적 신속하게 처리
- DPC는 공식적인 불만 처리 절차를 통해 3,218건의 불만을 해결<sup>3)</sup>

■ DPC의 지난 몇 년간 침해 신고 추세에 따르면, 공공 부문 기관과 은행이 가장 많은 침해 신고를 기록했으며 보험 및 통신사 역시도 상위 20위에 포함된 것으로 파악

- 특히 침해 사례 유형 중 무단으로 제공되는 개인정보가(우편, 이메일) 침해 사례의 50% 이상을 차지함

1) 다국적 기술기업들의 유럽 본부가 소재한 국가로, 아일랜드 개인정보 감독기구(DPC: Data Protection Commission)는 유럽 내 여러 국가에 영향을 미치는 개인정보 침해 사고와 관련 다수의 사례에서 선임 감독기구로 역할을 하는 등 유럽의 개인정보보호 규제 환경에서 중요성과 파급력이 큼

2) DPC. Annual Report 2023. 2024.5.29

3) 이 수치에는 2023년 이전에 접수된 불만이 포함

**표 1** 2023년 침해 사례의 특성(단위:건, %)

위반의 성격	전체수	비중
개인정보 무단 제공 - 우편물 오발송(Disclosure unauthorised - Postal Material to incorrect recipient)	2,255	33.69%
개인정보 무단 제공 - 이메일 오발송(Disclosure unauthorised - Email incorrect recipient)	1,203	17.97%
무결성 - 의도적이지 않은 변경 (개인정보 공개)(Integrity - unintentional alteration(Personal Data Disclosed))	602	8.99%
개인정보 무단 제공 - 기타(Disclosure unauthorised - Other)	571	8.53%
무단 접근 - 문서/기록(Unauthorised Access - Paper files/Documents /Records)	415	6.20%
가용성 - 사고 (개인정보 분실/파괴)(Availability - accidental (Loss /destruction of Personal Data))	396	5.92%

출처: DPC(2024.5)

#### **I DPC는 15억 5천만 유로에 달하는 행정 벌금을 부과하는 19건의 확정 결정을 내렸으며, 여기에는 여러 건의 견책 및 준수 명령이 포함**

- 2023년 5월, EU에서 미국으로의 데이터 전송과 관련하여 Meta Platforms Ireland Limited에 대한 GDPR 조사에 대한 종결을 발표
  - 이 결정으로 Meta Ireland에 12억 유로의 벌금을 부과하고, 사후 처리를 규정에 맞게 진행할 것을 명령함
- 2023년 9월, TikTok Technology Limited가 어린이 개인 데이터 처리와 관련해 규정을 위반했다고 판단하는 최종 결정을 발표
  - 이 결정으로 TikTok에 총 3억4천만 유로의 벌금을 부과하고, 사후 처리를 규정에 맞게 진행할 것을 명령함

#### **I 2023년 DPC는 더블린 순회법원에서 5개 조직에 행정 벌금 약 75만 유로에서 1만 5천 유로를 부과하기로 한 결정을 확정**

- 2023년 2월, DPC는 Bank of Ireland에 대한 조사에서 최종 결정을 내렸으며 이 조사는 Bank of Ireland 365 앱에 대한 일련의 데이터 침해와 관련이 있었음
  - 이 결정으로 행사된 시정 권한에는 견책, 75만 유로의 벌금, 사후 처리를 규정에 맞게 진행할 것을 명령함

- 2023년 1월 Centric Health에 대한 조사 결과에 따른 최종 결정을 발표했으며, 이 조사는 7만 명 이상의 환자 데이터를 보관 중이던 Centric의 환자 관리 시스템이 랜섬웨어 공격을 받으면서 시작됨
  - 이번 사태로 약 2,500명의 환자 데이터가 백업 없이 삭제되었으며, DPC는 Centric에 견책과 함께 총 46만 유로의 벌금을 부과

## (2) 정책/전략 및 주요 관심 영역

■ 2022년 DPC는 순환경제 및 기타 규정법(The Circular Economy and Miscellaneous Provisions Act 2022)에 따라 도입된 실무 강령에 대한 법정 협의를 포함한 37개 이상의 제안된 법안에 대한 의견을 제공

- 이 법률은 지방자치단체가 쓰레기 및 폐기물 관리 범죄를 예방, 조사, 감지 및 기소하기 위해 CCTV 및 바디 카메라와 같은 녹화 장치를 사용할 수 있는 명확한 법적 근거를 제공

■ DPC는 개인의 권리와 자유에 영향을 미칠 가능성이 있는 4개의 인터넷 플랫폼 프로젝트를 연기하거나 수정함

## 2. 영국 ICO<sup>4)5)</sup>

### (1) 2023년 주요 활동 및 성과(조사기간: 2023년 4월-2024년 3월)

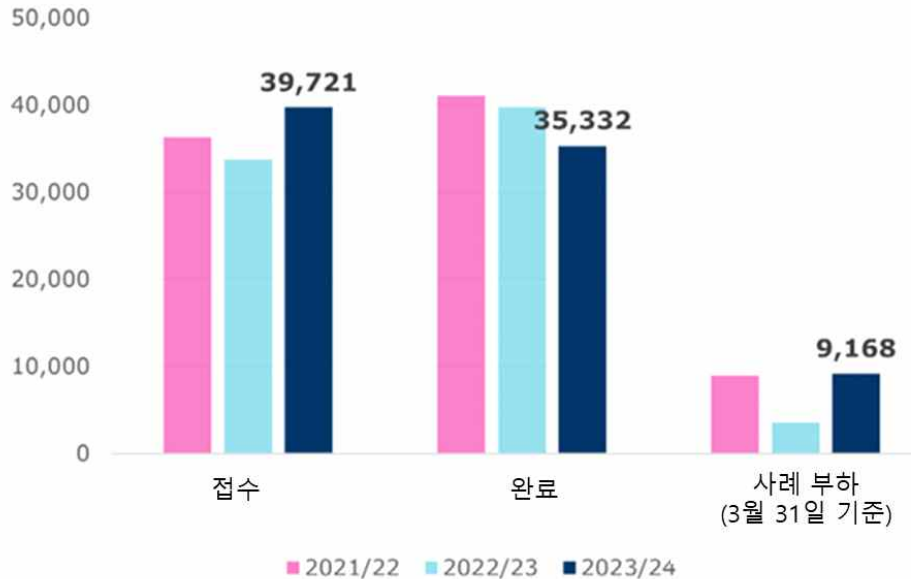
■ ICO는 39,721건의 데이터 보호 민원을 접수했으며 이는 전년보다 약 6,000건 증가한 수치지만, 민원의 범위와 분야는 전년과 거의 비슷한 수준을 유지

- 올해('23.4월~'24.3월)는 35,332건의 민원이 처리되었는데, 이는 전년 대비 약 4,400건 감소한 수치
- 또한 민원의 84.8%가 90일(ICO 목표 중 하나) 이내에 대응되었으며, 이는 전년 대비 상당히 개선된 결과, 99.7%는 6개월 내에 대응됨
- 민원 중 가장 많은 비중을 차지한 항목은 접근 권한(주체 접근 요청: the right of access (subject access requests))으로 응답자의 38.74%가 이를 이유로 민원을 접수하였으며, 이는 전년과 유사한 수준

4) 영국 정보위원회(Information Commissioner's Office, ICO)는 유럽 내에서 행정처분을 강화하고 있는 유럽 감독기관으로 부상

5) ICO, Information Commissioner's Annual Report and Financial Statements 2023/24, 2024.7.23

**그림1** 연도별 데이터 보호 민원 처리 건수(단위: 건)



출처 : ICO(2024.7)

## (2) 정책/전략 및 주요 관심 영역

ICO는 개인정보 위반에 대해 주로 견책을 주는 방식을 고수하며, 특히 사람들이 가장 큰 피해를 입을 위험이 있는 경우나 더 심각한 위반에 대해서만 집행 통지나 벌금을 부과

- 올해 가장 큰 벌금은 2023년 4월 TikTok에 부과된 1,270만 파운드였으며, 에너지 회사도 불법 마케팅 전화에 대해 25만 파운드의 벌금을 부과한 이력이 있음

ICO는 DSIT<sup>6)</sup>가 DPDI 법안<sup>7)</sup>을 준비를 지원하겠다는 입장을 발표

- 이 법안은 영국 총선 전에 폐기되었지만, 새 정부의 디지털 정보 및 스마트 데이터 법안(new Government's Digital Information and Smart Data Bill)에서 관련 조항이 포함될 가능성에 대해 예의주시하고 있는 상황

6) 영국의 과학혁신기술부(DSIT: Department for Science, Innovation and Technology)

7) 데이터 관련 개인정보 보호 및 디지털 정보법안(Data Protection and Digital Information Bill, DPDI): 2023년 11월, 영국 의회는 스마트 데이터 관련 개인정보 보호 및 디지털 정보법안(Data Protection and Digital Information Bill, DPDI)을 상정. 에너지, 통신, 모기지를 포함한 7개 부문에서 스마트 데이터 체계(Smart Data Scheme)를 구축하는 것이 법안의 내용임. 이는 공인된 제3자 서비스 제공자(TPP)가 고객 데이터를 안전하게 공유 받고 한층 더 혁신적인 맞춤 상품이나 서비스를 추천하는 것을 가능하게 함

### 3. 프랑스 CNIL<sup>8)9)</sup>

#### (1) 2023년 주요 활동 및 성과

■ 2023년 CNIL에 접수된 민원 건수가 증가하여 총 16,433건이 접수되었으며(2022년 대비 +35%), 2년 연속 접수된 민원 건수에 대해 모두 처리 완료

- 또한 전용 온라인 서비스를 통해 간접 접근 권한(특정 은행 또는 경찰 파일에 대한 액세스 기능)에 대한 요청을 20,810건 받았으며, 이는 1년 만에 217% 증가한 수치

■ CNIL은 적극적인 규제 활동을 통해 총 340건의 조사를 실시했으며, 대부분 현장과 온라인에서 제기된 문제를 근거로 이루어짐

- 2023년은 작년에 비해 2배에 달하는 42건의 제재가 내려졌으며, 이 중 36건은 총 8,900만 유로에 달하는 벌금을 부과
  - CNIL 의장은 데이터 보호 규정을 위반한 조직에 대해 168건의 공식 통지와 33건의 법적 의무 알람을 발표
- 또한 2023년은 CNIL 규제활동의 간소화 절차가 실제로 시작된 해로, 이를 통해 계속 증가하는 민원에 훨씬 더 효과적으로 대응할 수 있었음
  - 그 결과 전체의 절반이 넘는 24건의 제재가 이 절차에 따라 내려짐

#### (2) 정책/전략 및 주요 관심 영역

■ 2023년 CNIL은 인공지능에 중점을 둔 지원 전략을 강화하며, 경제적 또는 혁신 잠재력이 높은 기업에 대한 지원 확대

- CNIL은 부문별 지원 및 개별 지원(2023년에 접수된 1,651건의 자문 요청)을 제공하는 것 외에도 보건 부문에 대한 ▲5개의 새로운 가이드 ▲4개의 참조 문서 ▲2개의 권장 사항 및 2개의 참조 방법론 등 13개의 새로운 참조 문서를 작성
- 마지막으로, "GDPR Days"(Journées RGPD)의 일환으로 랭스, 렌, 마르세유 및 툴루즈 등 여러 지역을 순회하며 전문가와 학생들과 간담회 주도

8) 개인정보보호법 위반사례 조사·처분과 관련하여 활발한 활동을 전개하는 국가로, 프랑스의 개인정보 감독기구(CNIL: Commission nationale de l'informatique et des libertés)는 특히 빅테크에 대한 대규모 과징금 처분으로 주목받음

9) CNIL, The CNIL publishes its annual report for 2023, 2024.4.23

**그림2** 2023년 CNIL 주요 활동(단위: 건, 명)



출처 : CNIL(2024.4)

**출처 |**

1. DPC, Annual Report 2023, 2024.5.29.
2. ICO, Information Commissioner's Annual Report and Financial Statements 2023/24, 2024.7.23.
3. CNIL, The CNIL publishes its annual report for 2023, 2024.4.23.



# 2024년 주요 개인정보보호 실태 서베이 보고서 분석



## [목 차]

1. CISCO - 개인정보보호 벤치마크 연구
2. IBM - 2024년 데이터 유출 비용 보고서
2. Protiviti Oxford - 2030년 개인정보 보호의 미래 전망

### 1. CISCO<sup>10)</sup> - 개인정보보호 벤치마크 연구<sup>11)</sup>

발표 시점: 2024년 1월  
조사 시점: 2023년 여름  
조사 대상: 12개국 2,600명 이상의 보안 전문가

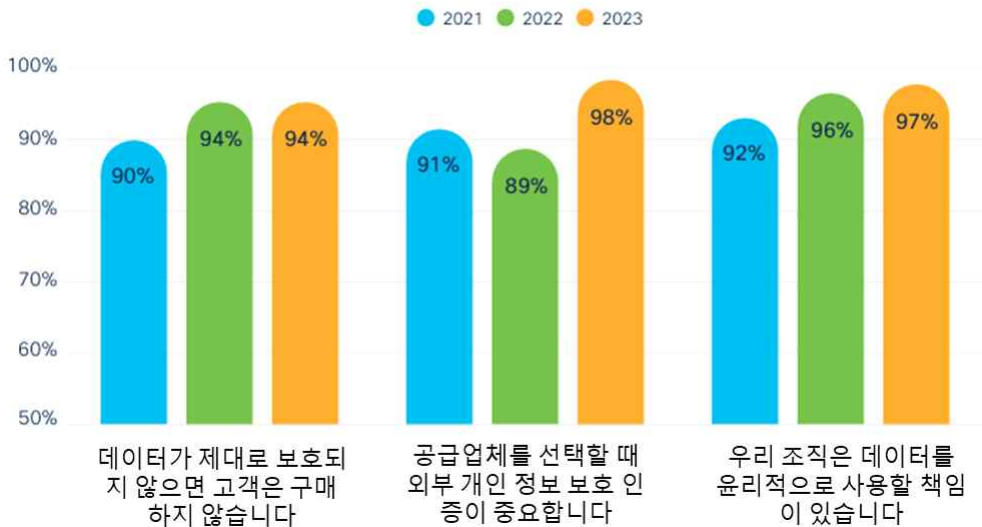
#### ■ 설문조사결과, 조직들은 데이터를 신뢰할 수 있는 업체에서 구매하기를 더욱 선호하며 응답자의 94%는 고객 데이터를 적절히 보호하지 않으면 구매하지 않겠다고 응답

- 또한 응답자의 98%는 ▲ISO 27701, 아시아태평양경제협력체(APEC)의 국경 간 개인정보 보호 규칙(Cross-Border Privacy Rules) ▲유럽연합(EU)의 구속력 있는 기업 규칙(Binding Corporate Rules)과 같은 개인정보보호 인증이 구매 과정을 결정하는 중요한 요소라고 응답
- 기업 조직은 신뢰할 만한 개인정보보호 인증이고객 신뢰에 중요하다는 것을 인식하고 있었으며, 거의 모든 조직(97%)이 데이터를 윤리적으로 사용할 책임이 있다고 생각한다고 응답
  - 이는 지난 3년간의 설문조사에서 가장 높은 수준

10) 1984년 샌프란시스코에 설립한 미국의 정보 통신 회사. 네트워크 설비들을 제조 · 판매하며, 다양한 네트워킹 솔루션과 서비스 제공

11) Cisco, 2024 Data Privacy Benchmark Study, 2024.1.29.

**그림3** 고객 신뢰에 대한 개인정보 보호의 중요성(단위: %)



출처: CISCO(2024.1)

#### Ⅰ 또한 올해 벤치마크 연구에서는 조직은 일반 소비자보다 개인정보 보호법을 더 강력히 지지한다고 응답<sup>12)</sup>

- 전체 기업 응답자의 80%는 개인정보 보호법이 조직에 긍정적인 영향을 미쳤다고 평가했으며, 14%는 중립적, 6%만이 부정적인 영향을 미쳤다고 응답
  - 이는 ▲데이터 카탈로그 작성(cataloging data) ▲제어 구현(implementing controls) ▲사용자 요청 응답(responding to user requests) 등 개인정보 보호 규정 준수와 관련된 상당한 노력과 비용을 투자한 결과로 분석됨
- 또한 이런 결과는 아시아(78%) 유럽(80%) 미주(83%) 등 전 세계적으로 긍정적인 영향이 동일하게 나타남
  - 국가별로는 ▲중국(91%) ▲인도(88%) ▲독일(86%) ▲미국(86%) 순으로 긍정적 평가 비율이 높았음

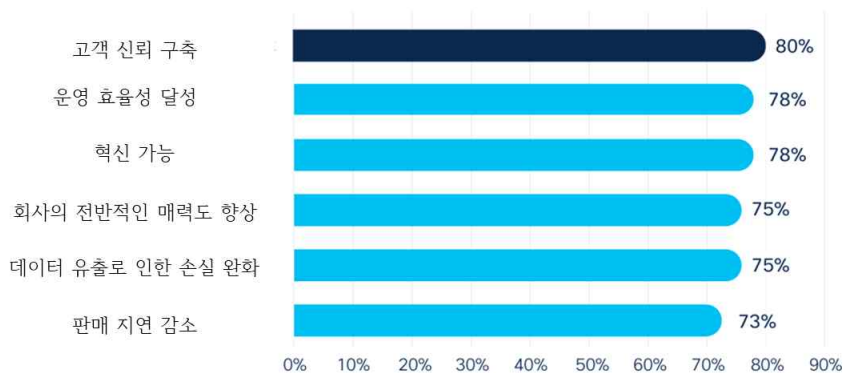
12) 정부, 조직, 개인 모두가 개인 데이터를 보호하는 데 역할을 해야 하지만, Cisco 2023 소비자 개인정보 보호 설문조사 응답자의 50%는 정부가 주도적으로 참여하기를 원한다고 응답

**그림4** 국가별 개인정보 보호법이 조직에 미치는 영향(단위: %)

출처: CISCO(2024.1)

### I 기업은 개인정보 보호 투자와 비즈니스 혜택 사이에 연관성을 점점 더 인식하고 있으며, 특히 브랜드 신뢰도와 충성도를 구축하는 데 유용하다고 느끼고 있음

- 응답자의 70% 이상이 개인정보 보호 투자를 통해 6가지 비즈니스 혜택 영역<sup>13)</sup>에서 “상당하다” 또는 “매우 중요하다”라고 응답
  - 특히 ‘고객 충성도 및 신뢰 구축’은 가장 높은 응답 비율(80%)로, 지난 2년간 71%, 75%에서 꾸준히 증가한 수치를 기록

**그림5** 개인정보 보호 투자가 브랜드 로열티와 신뢰에 미치는 영향(단위: %)

출처 : CISCO(2024.1)

13) 6가지 영역은 ▲판매 지연 감소 ▲데이터 유출로 인한 손실 완화 ▲혁신 가능 ▲운영 효율성 달성 ▲고객 신뢰 구축 ▲회사의 전반적인 매력도 향상 등임

## 2. IBM - 2024년 데이터 유출 비용 보고서<sup>14)</sup>

발표 시점: 2024년 7월

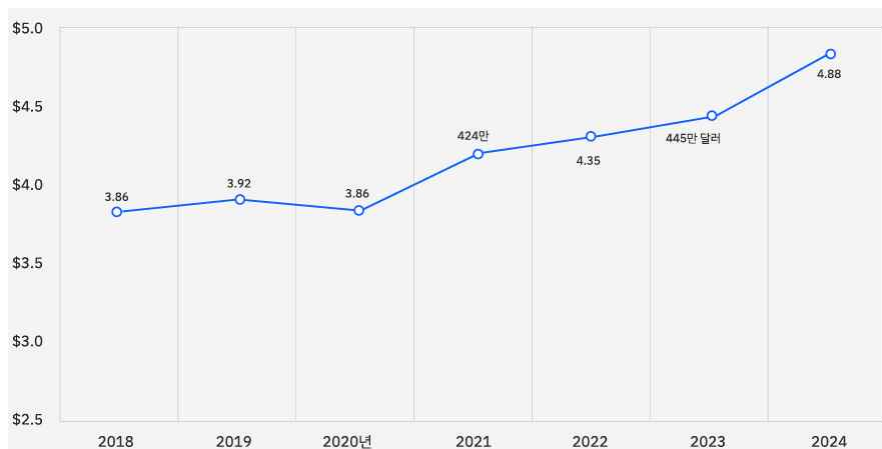
조사 시점: 2023년 3월~2024년 2월

조사 대상: 데이터 유출 피해 입은 604개 조직

**전 세계 데이터 유출로 인한 평균 비용은 1년 동안 10% 증가하여 488만 달러에 달했고, 이는 팬데믹 이후 가장 큰 폭의 증가**

- 그 중 비즈니스 중단과 유출 후 대응 조치가 연간 비용 증가의 주요 원인으로 분석됨

**그림6** 데이터 유출의 글로벌 평균 총 비용(단위: 달러, 미화 100만 달러 단위 기재)



출처 : IBM(2024.7)

**공격자가 유출된 자격 증명을 사용했을 때 발생한 평균 유출 비용은 481만 달러에 달했으며, 이는 연구 대상 유출 사례 중 16%에서 발생**

- 또한 피싱과 도난 또는 손상된 자격 증명이 가장 많이 발생한 공격 벡터 1, 2위를 차지했으며, 이 두 유형은 모두 가장 비용이 많이 드는 유형으로 상위 4위 안에 포함됨

14) IBM, cost of a data breach report 2024, 2024.7.31.

**그림7** 최초 공격 수단별 데이터 유출의 비용 및 빈도(단위: 달러, 미화 100만 달러 단위 기재)

출처 : IBM(2024.7)

### 3. Protiviti Oxford – 2030년 개인정보 보호의 미래 전망<sup>15)</sup>

발표 시점: 2024년 11월

조사 시점: 2024년 8월~2024년 9월

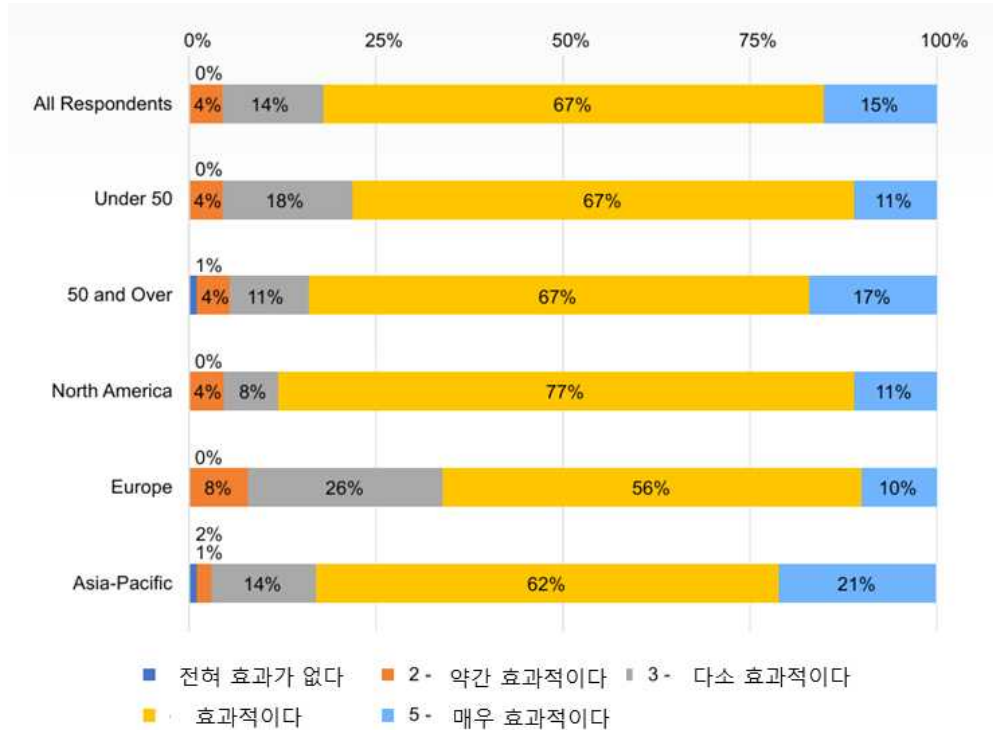
조사 대상: 북미, 유럽, 아시아 지역의 이사회 구성원, CEO 250명

#### I 대기업 C레벨급의 임원진 78%가 개인정보 유출에 대해 심각하게 우려하고 있음

- 특히 노령 및 북미 기업 리더가 이 문제에 대해 가장 불안해하는 것으로 나타났으며, 50세 이상의 84%와 북미에 본사를 둔 임원의 89%가 상당한 우려를 표명

15) Protiviti Oxford, Executive Outlook on the Future of Privacy, 2030. 2024.11

**그림8** 자사 데이터 관리 관행 및 개인정보보호 보장도(단위: %)



출처 : Protiviti Oxford(2024.11)

## I 대기업 C레벨급의 임원진은 자사의 데이터 보안 및 개인정보 보호 관행에 대해 명확하게 자신하고 있지 않은 것으로 조사

- 응답자의 86%는 회사가 고객 데이터를 보호하기 위해 최선을 다하고 있다고 확신하거나 매우 확신한다고 응답
- 응답자의 82%는 조직의 현재 데이터 관리 관행이 포괄적인 데이터 개인정보 보호를 보장하는 데 효과적이라고 믿고 있었음
- 또한 75%는 회사가 2030년까지 자금 및 리소스 측면에서 개인정보 보호 기능을 적절히 처리할 준비가 되었다고 응답

출처 |

1. Cisco, 2024 Data Privacy Benchmark Study, 2024.1.29.
2. IBM, cost of a data breach report 2024, 2024.7.31.
3. Protiviti-Oxford, Executive Outlook on the Future of Privacy, 2030. 2024.11

# 미국 연방거래위원회(FTC)의 개인정보보호 및 정보보안 관련 집행 트렌드 분석



## [목 차]

### 1. 개요

### 2. FTC의 개인정보 보호 및 정보보안 관련 집행 사례

- (1) 아동 개인정보 보호
- (2) 건강 개인정보 보호
- (3) 일반 개인정보 보호
- (4) 데이터 보안 관행 및 침해사고 대응
- (5) 서비스 제공자 및 제3자 접근통제
- (6) 근로자 데이터 관리
- (7) AI 거버넌스

### 3. 결론

#### 1. 개요

■ 국제개인정보보호전문가협회(IAPP)는 '18년 10월부터 '24년 4월까지 개인정보 및 정보보안 관련 미국 연방거래위원회(FTC)가 내린 총 67건의 집행을 분석('24.5.)<sup>1)</sup>

- FTC는 소비자 보호와 공정 거래 및 경쟁 강화 업무를 담당하는 독립적인 법 집행 기관으로서 개인정보보호와 관련된 각종 활동을 수행
  - FTC는 법적 권한을 통해 신기술과 비즈니스 모델의 발전과 함께 제기되는 개인정보보호 문제를 포함해 시장에서 불공정하거나 기만적인 관행을 금지 및 제재

■ IAPP는 FTC의 법 집행 사항을 분석함으로써 개인정보 및 정보보안과 관련된 주요 동향을 개괄하고 기업의 규정 준수와 사례 연구를 위한 심층적인 정보를 제공할 수 있을 것으로 기대

- IAPP에 따르면 FTC는 역사적으로 개인정보 및 정보보안 규정 준수를 위한 명확한 지침을 제공하기보다는 실제 법 집행을 통해 FTC가 비합리적인 관행으로 간주하는 사례를 제시

1) IAPP, FTC enforcement trends: From straightforward actions to technical allegations, 2024.05.

- 이에 IAPP는 개인정보 및 정보보안 관련 FTC의 집행 사례를 7개의 주요 분야별로 분석함으로써 기업들이 규정 준수를 위해 취할 수 있는 조치를 안내
- 7개 분야는 ▲아동 개인정보 보호 ▲건강 개인정보 보호 ▲일반 개인정보 보호 ▲데이터 보안 관행 및 침해사고 대응 ▲서비스 제공자 및 제3자 접근통제 ▲근로자 데이터 관리 ▲AI 거버넌스로 구성

## 2. FTC의 개인정보 보호 및 정보보안 관련 집행 사례

### (1) 아동 개인정보 보호

■ FTC는 '18년 10월 이후 아동온라인개인정보보호법(COPPA, Children's Online Privacy Protection Act)에 따라 아동 개인정보보호와 관련해 총 14건의 법 집행을 내렸으며, '22년 12월 인기 게임사 Epic Games에 부과한 제재가 대표적

- FTC는 소송에서 Epic Games가 마케팅 및 사용자 설문조사를 통해 사용자 기반의 상당수가 아동임을 알고 있었음에도 아동 개인정보 수집 시 부모 또는 보호자에 대한 통지 및 동의 요건을 준수하지 않았다고 주장
- Epic Games는 게임 〈Fortnite〉 서비스 과정에서 부모의 자녀 개인정보 삭제 요청 시 혼란스럽고 불합리한 절차를 만들고 때로는 부모의 요청을 존중하지 않았으며, 아동과 청소년이 낯선 사람과 소통할 수 있도록 허용하여 괴롭힘의 위험을 높였음
- Epic Games는 또한 게임 내 구매를 유도하기 위한 다크패턴\*을 사용해 아동이 부모나 카드 소지자의 동의 없이 게임 내 콘텐츠를 빈번하게 구매하는 결과를 초래했으며, 이러한 관행에 대한 100만 건 이상의 사용자 불만과 여러 직원의 우려를 무시
- \* 소비자의 구매 결정을 왜곡하기 위해 교묘하게 설계된 장치
- FTC는 Epic Games의 COPPA 규정 위반에 대하여 2억 7,500만 달러를 부과하는 한편, 다크패턴 청구 관행에 대하여 소비자 환불을 위해 2억 4,500만 달러를 추가로 지급하라는 행정명령을 내림

■ IAPP는 Epic Games 사례를 포함한 FTC의 법 집행 사항을 분석해 아동 사용자를 대상으로 온라인 서비스나 제품을 제공하는 기업에 다음과 같은 권고사항을 제시

- (사용자 통지 및 선택) 아동 개인정보의 수집 및 사용 사실을 부모에게 알리고 개인정보 수집 전 검증 가능한 방식으로 부모나 보호자 동의를 획득해야 하며, 아동의 개인정보는 기본적으로 비공개로 유지



- **(데이터 거버넌스)** 데이터 최소화 및 저장 관련 엄격한 정책을 수립하고 부모의 요청이 있거나 아동의 계정이 비활성 상태인 경우 해당 데이터를 삭제하며, COPPA에 따라 유효한 통지 및 동의 없이 아동 개인정보를 이용해 알고리즘을 훈련해서는 안 됨
- 다양한 연령층의 고객 대상 서비스의 경우, 아동과 일반 사용자 간 커뮤니케이션 채널을 제한하고, 아동용 게임에서 요금 청구를 승인하기 위해 부모의 동의를 요구하는 앱 내 구매 프로토콜을 구현

## (2) 건강 개인정보 보호

**I FTC는 웨어러블 기기와 개인 건강 관련 모바일 앱이 보편화되면서 개인 건강정보 관련 법 집행을 강화하는 추세로, '23년 6월에는 임신 주기 추적을 지원하는 모바일 앱 Easy Healthcare과 민감한 건강 정보 공유를 이유로 제기한 소송을 합의로 종결**

- Easy Healthcare는 월경 주기, 임신 가능성, 임신과 관련된 개인정보를 수집하고 사용자가 다른 앱에서 데이터를 가져올 수 있는 모바일 앱 Premom을 개발
- FTC에 따르면 Easy Healthcare는 건강침해고지 규정(Health Breach Notification Rule, HBNR)을 위반하여 사용자의 민감한 개인정보를 제3자와 무단으로 공유하고 이를 소비자에게 알리지 않았음
- 또한 소프트웨어 개발 키트와 같은 제3자 자동 추적 도구를 사용하여 발생하는 개인정보 보호 및 보안 위험 해결을 위한 접근통제도 구현하지 않았음
- FTC는 Easy Healthcare에 10만 달러의 민사 과징금을 부과하고 광고 목적으로 사용자의 건강 개인정보를 제3자와 영구적 공유를 금지하며, 다른 목적으로 건강 데이터 공유 전 사용자 동의를 얻기로 합의

**II IAPP는 건강 관련 개인정보 보호를 강화하는 FTC의 법 집행 동향을 반영해 개인 건강정보를 수집 또는 처리하는 기업들에 다음과 같은 권고사항을 제시**

- **(사용자 통지 및 선택)** 건강 서비스 기업이 데이터를 수집·보관·사용·공개하는 모든 목적을 밝히고, 소비자의 건강 정보를 수집·사용 및 제3자에게 공개하기에 앞서 소비자의 명시적 동의를 확보
- **(데이터 공개)** “판매”에 제3자 광고주 및 플랫폼과 개인정보 공유가 포함될 수 있다고 가정하고, 소프트웨어 개발 키트와 같이 정보공개를 가능하게 하는 기술을 특히 염두에 두고 제3자의 접근 및 사용을 모니터링 및 제어해 소비자 건강 정보를 보호하며, 개인 식별 정보의 무단 공개 시 소비자 및 필요 시 FTC와 언론에 통보

- **(데이터 관리)** 건강 관련 데이터를 광고 플랫폼과 공유되는 검색 질문, 페이지 탐색 등까지 포함하도록 광범위하게 정의하여 운영하고, 민감정보를 암호화하지 않은 공공 서버에 저장하거나 개인 식별 정보와 함께 저장하지 않도록 주의하며, 제3자로부터 보안 취약점 경고를 받을 시 즉각 시정

### (3) 일반 개인정보 보호

#### I 일반 개인정보와 관련해서도 FTC의 법 집행이 다수 이루어졌으며, '21년 5월 사진저장 사업자 Everalbum의 개인정보 침해에 대한 제재가 대표적 사례

- Everalbum은 소비자가 사진과 동영상을 클라우드 서버에 업로드하도록 하고 안면 인식 기술을 사용해 각 사진에 등장하는 개인별로 사진을 그룹화했으며, 대부분 사용자는 안면 인식 기술을 인지하지 못했고 해당 기능을 비활성화할 수 없었음
- Everalbum은 안면 인식 기능을 비활성화하지 않은 사용자의 사진을 이용해 자체 안면 인식 기술을 훈련했으며, 계정 비활성화를 요청한 사용자의 사진과 동영상을 삭제하지 않아 개인정보 보호 정책을 위반
- 이에 FTC는 Everalbum에 생체정보 관련 사용 정책을 공개하고 해당 정보를 제공한 사용자의 명확한 동의를 받을 것과 계정을 비활성화한 사용자 데이터로 훈련된 정보와 모델을 삭제할 것을 요구
- Everalbum은 FTC가 안면 인식 기술 규제에 초점을 맞춘 최초의 사례로, FTC는 '24년 4월까지 총 5건의 안면 인식 기술 관련 법 집행을 진행

#### II IAPP는 금융, 광고 기술 및 기타 개인정보를 포함하는 일반 개인정보 관련 법 집행 사례를 토대로 다음과 같은 권고사항을 제시

- **(사용자 통지 및 선택)** 사진과 동영상을 포함한 개인정보의 인적 검토에 대하여 고객에게 알려거나 동의를 확보하고, 개인정보를 사용·판매·공유할 수 있는 모든 목적을 명확히 공개하며, 모든 형태의 소비자 옵트아웃을 존중하고, 알고리즘이나 기타 데이터 세트 훈련을 위해 민감한 개인정보 사용 시 명시적인 적극적 동의를 획득
- **(데이터 공개)** 정확한 지리적 위치 데이터를 추적·제공·판매·공유하는 경우, 민감한 위치 목록 제공 등 제3자가 소비자를 식별하거나 민감한 위치까지 추적하는 행위를 금지하는 기술적 통제 수단을 채택
- **(데이터 관리)** 불필요한 데이터 삭제나 계정 비활성화를 요청한 사용자로부터 수집된 개인 데이터 삭제 등 목적 제한 및 통지, 삭제 정책을 수립하고, 서비스의 기본 설정을 평가해 개인정보 보호 정책과 일치하는지 확인

#### (4) 데이터 보안 관행 및 침해사고 대응

■ FTC는 데이터 보안 및 침해사고 대응에서 구체적인 보안 의무를 규정해 법을 집행하고 있으며, 데이터 침해사고를 초래한 Uber Technologies에 대한 제재가 대표적

- Uber는 '14년 5월 사이버 공격으로 운전자 개인정보 침해 사건을 겪은 데 이어 '16년에는 사내 엔지니어가 코드 공유 웹사이트 Github에 게시한 키를 획득한 외부 공격자에 의해 타사 클라우드 서버에 저장된 소비자 데이터가 유출되었으며, 유출 정보에는 수천만 명의 Uber 승객과 운전자 이름, 이메일 주소, 전화번호, 운전면허증 번호가 포함
- FTC는 Uber가 승객과 운전자 정보에 대한 직원의 접근을 철저히 모니터링하고 타사 클라우드 서비스에 저장된 개인정보를 보호하기 위해 합리적으로 조치했다는 기만적 주장을 했으며 정보 유출 시 피해자에 사실을 알려야 하는 법적 의무도 회피했다고 지적
- FTC는 Uber에 소비자와 관련된 모든 데이터 및 제3자 감사기관의 평가 보고서를 제출할 것을 요구했으며, 소비자 정보에 대한 무단 접근과 관련된 버그바운티 프로그램에 대한 기록도 보관하도록 명령

■ IAPP는 데이터 보안 및 침해사고 대응에서 기업들에 다음과 같은 권고사항을 제시

- **(사용자 지원)** 침해 계정에 대한 우려 사항에 적시 대응할 수 있도록 고객 지원을 적절히 유지하고 소비자 계정정보 변경이나 계정에 신규 기기 추가 시 보안 경고를 전송
- **(보안 조치)** 개인정보에 접근할 수 있는 모든 계정에 다중 인증을 구현하고, Github와 같은 보안이 약한 플랫폼에 주요 데이터베이스 정보 저장을 금하며, 네트워크 취약점 스캐닝과 침투 테스트를 시행하고 침입 탐지 및 방지 시스템을 구현
- **(침해사고 대응)** 침해사고 발생 직후 및 적어도 12개월마다 개인정보 보안과 기밀성, 무결성 위험에 대응한 보호장치가 충분한지 평가하고, 결과에 따라 기존 정보보안 프로그램을 보완

#### (5) 서비스 제공자 및 제3자 접근통제

■ 현대의 복잡한 데이터 생태계 하에서 FTC는 직원이나 고객 개인정보의 제3자 공유 시 개인정보 관리를 강조하고 있으며, '18년 9월 휴대전화 제조업체 BLU Products에 내린 제재에서도 제3자 서비스 제공업체로 인해 발생한 보안 취약점에 대해 책임을 부과

- BLU Products는 중국에 있는 제3자 서비스 제공업체 ADUPS Technology와 계약해 자사 기기의 보안 및 운영체제 업데이트를 제공

- FTC에 따르면 BLU Products는 ADUPS의 보안 프로세스를 제대로 감독하지 않았으며, 그 결과 소비자가 알지 못하는 민감한 개인정보 수집 및 소비자 기기의 보안 취약점을 초래
- FTC는 BLU Products 및 동 기업의 소유자 겸 사장인 Samuel Ohev-Zion을 소송 당사자로 지명하고 합의안에서 의무적 데이터 보안 프로그램의 수립을 요구

## I IAPP는 서비스 제공자 및 제3자 접근통제에서 다음과 같은 권고사항을 제시

- **(제3자 보안 정책 수립)** 제3자 감독을 위한 보안 정책을 채택 및 이행하고, 개인정보를 취급하는 제3자에 대한 정기적 재평가를 포함하여 서비스 제공업체 및 서비스 제공업체 감독을 담당할 내부 책임자를 지정
  - 고객 개인정보에 대한 내외부 위험을 파악하고, 해당 위험을 통제하기 위한 안전장치를 정기적으로 모니터링 및 평가하여 조정
  - 제3자 개발업체에 대한 위험 평가를 수행하고 위험 완화 방법을 개발하며, 특히 사용자가 비공개로 지정한 데이터에 대한 접근을 허용하기에 앞서 개발업체와 제품을 검토
- **(서비스 제공자에 대한 보안 요구사항)** 서비스 제공자에게 개인정보 보호를 위한 적절한 조치를 이행하도록 계약을 통해 요구하고, 개인정보 침해사고를 해결하고 조사하기 위한 정책과 절차의 수립 및 시행을 요구

## (6) 직원 데이터 관리

### I 직원과 계약업체의 개인정보 및 데이터 접근으로 인해 기업에 대한 책임이 발생할 수 있으며, FTC는 '23년 6월 직원과 계약업체에 의한 고객 개인정보 침해를 초래한 Ring에 제재 결정을 내림

- Ring은 '18년 아마존이 인수한 가정용 보안 카메라 기업으로, 소비자의 가정 내 개인 공간을 모니터링하는 카메라 등 인터넷 연결 기능을 갖춘 액세서리 및 서비스를 판매
- Ring은 내부 직원에게 고객의 영상기록에 대한 광범위한 접근 권한을 허용했으며, 동의 없이 고객 영상을 사용해 알고리즘을 학습하고 합리적인 보안 관행을 구현하지 않았음
  - Ring의 모든 직원과 수백 명에 달하는 제3자 계약업체는 별도의 허가 없이 카메라의 모든 동영상에 접근할 수 있었으며, 한 직원은 욕실과 침실 같은 사적 공간에 설치된 여성 사용자의 영상기록 수천 개를 열람한 것으로 드러남
- FTC는 이번 사건에 대하여 기업이 개인정보 보호 정책에 데이터 수집 목적을 숨겨서는 안 된다고 강조하고, 소비자 데이터에 접근할 수 있는 직원에 대한 통제와 모니터링을 의무화할 것을 요구
  - FTC는 링에 대하여 '18년 3월 이전까지의 영상기록과 해당 데이터를 바탕으로 개발된

모델과 알고리즘 삭제 및 개인정보보호 및 데이터 보안 프로그램의 구현을 요구

## Ⅱ IAPP는 데이터에 접근할 수 있는 직원 관리를 위해 다음과 같은 권고사항을 제시

- (보안 정책의 수립) 직원 교육을 포함하는 서면 정보보안 정책을 수립하고, 기업이 수집하는 개인정보의 종류, 수집 목적, 정보 삭제 시기 등을 명시한 일정을 문서화하여 관리
  - 정보보안 프로그램을 담당할 내부 책임자를 지정하고, 소비자 데이터에 접근할 수 있는 직원의 권한을 직무 수행에 필요한 범위로 제한하거나 직원의 접근을 모니터링하고 탐지할 수 있는 조치를 시행

## (7) AI 거버넌스

### Ⅱ 최근 FTC는 AI 기술을 이용한 소비자 피해에 주목하면서 '24년 3월까지 총 5건의 법 집행을 통해 AI 사용을 규제했으며, '23년 12월 Rite Aid에 부과한 제재가 대표적

- 대형 약국 체인인 Rite Aid는 AI 기반 안면 인식 기술과 자동 생체인식 탐지 시스템을 사용하여 절도 및 기타 문제 행위에 가담할 가능성이 있다고 여겨지는 고객을 식별
- FTC에 따르면 Rite Aid는 '12년부터 '20년까지 8년에 걸쳐 해당 기술을 사용해 고객에게 굴욕감과 기타 피해를 초래했으며, 유색인종에게 차별적으로 적용되거나 특정 고객을 절도범으로 잘못 식별하는 사례도 발생
- FTC는 Rite Aid가 고객에게 발생할 수 있는 예측 가능한 피해를 예방하기 위한 합리적인 조치를 취하지 못했으며, 고객에게 안면 인식 기술 사용에 대해 알리지 않았고 직원들에게도 기술 사용 사실을 비밀로 하도록 지시했다고 지적
  - IAPP는 Rite Aid가 초래한 소비자 피해의 상당 부분이 AI 기술 사용과 관련된 위험 평가와 배포 전후의 정기적인 정확성 평가와 품질 모니터링, 운영을 담당하는 직원 교육과 감독을 통해 예방, 완화 또는 시정할 수 있었다고 강조
- 이에 FTC는 5년 동안 Rite Aid에 감시용 안면 인식 기술의 사용을 금지하기로 했으며, Rite Aid는 이 결정을 수용

### Ⅱ IAPP는 '24년 1월 FTC가 기술 블로그를 통해 AI 기업에 강조한 개인정보 보호 및 기밀 유지 요구 사항<sup>2)</sup>을 토대로 AI 거버넌스에서 다음과 같은 권고사항을 제시

- 안면 인식 기술과 같은 AI 기술 사용 시 고객에 대한 통지, 동의 획득, 체계적 위험 평가, 옵트아웃 존중과 같은 개인정보 보호 원칙을 준수

2) FTC, AI Companies: Uphold Your Privacy and Confidentiality Commitments, 2024.01.09.

- 소비자에게 안면 인식 기술과 같은 자동화 의사결정 시스템의 결과물에 관련된 불만 사항을 제출할 수 있는 수단을 제공
- 사용자가 기능 활성화 옵션을 선택하지 않은 이상 사용자의 콘텐츠에 안면 인식 기술을 자동으로 적용하지 않도록 주의
- 유효한 통지 및 동의 없이 아동 개인정보나 고객 영상기록과 같은 민감한 개인정보를 이용해 알고리즘을 훈련해서는 안 되며, 적절한 근거 없이 AI나 알고리즘 사용 관련 진술을 하지 않도록 주의
- AI 시스템 품질에 대하여 사용 전후의 정확도 테스트, 거짓 양성 추적, 입력 품질 모니터링, 소비자 특성에 따른 오류 발생 위험 등을 포함하는 통제 정책을 수립

### 3. 결론

**I FTC의 법 집행 사례를 살펴보면 FTC는 개인정보 보호 및 정보보안과 관련된 접근방식과 집행 우선순위 결정에서 지속적인 발전을 보였으며, 특히 ▲아동 ▲건강 ▲금융 정보와 같은 민감한 데이터 범주 보호에 주력하는 추세를 확인 가능**

- FTC는 또한 AI와 다크패턴, 광고기술 도구와 관련된 법 집행을 통해 신흥 산업 규제에 필요한 기술 전문성을 입증했으며, 제3자 접근 및 서비스 제공자로 개인정보와 정보보안 규제 범위를 확장
- FTC는 '24년 3월 발표한 '2023 개인정보 및 정보보안 업데이트'<sup>3)</sup>에서도 '21~'23년 기간 ▲AI ▲건강 정보 ▲아동 개인정보 ▲위치정보 등과 관련된 소비자 개인정보 보호 및 위협 완화에 중점을 두고 있음을 보여줌
  - 특히 AI 기술과 관련해 FTC는 머신러닝 및 알고리즘을 개발하고 배포하기 위해 아동을 포함한 소비자 개인정보를 수집, 보유 또는 사용하는 행위를 규제하는 한편, Rite Aid 사례에서 확인되듯 고객 감시 목적의 안면 인식 기술 사용을 금지
  - FTC는 소비자의 민감한 개인정보 보호 역시 최우선 과제로 설정하고 있으며, 아동 개인정보를 수익화하는 조건으로 서비스 접근을 허용하는 기업 행위를 제한하기 위한 COPPA 규칙 업데이트를 제안하기도 했음

3) FTC, FTC Releases 2023 Privacy and Data Security Update, 2024.03.28.

## 출처 |

1. FTC, Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges, 2022.12.19.
2. FTC, Easy Healthcare Corporation, U.S. v., 2023.06.26.
3. FTC, FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology, 2021.05.07.
4. FTC, Uber Technologies, Inc., In the Matter of, 2018.10.29.
5. FTC, BLU Products and Samuel Ohev-Zion, In the Matter of, 2018.09.11.
6. FTC, Ring, LLC, 2024.04.23.
7. FTC, Rite Aid Corporation, FTC v., 2024.03.08.
8. FTC, FTC Releases 2023 Privacy and Data Security Update, 2024.03.28.
9. IAPP, FTC enforcement trends: From straightforward actions to technical allegations, 2024.05.

# 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, CMA와 온라인 선택 아키텍처의 유해한 설계 사례와 개인정보 악영향 고찰
24	12월 1호	해외 주요 개인정보 감독기관 연례보고서
25	12월 2호	2024년 주요 개인정보보호 실태 서베이 보고서 분석
26	12월 3호	미국 연방거래위원회(FTC)의 개인정보보호 및 정보보안 관련 집행 트렌드 분석



# 2024 개인정보보호 월간동향분석

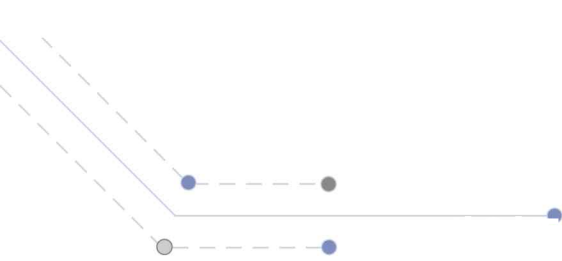
『2024 개인정보보호 월간동향분석 보고서』는  
개인정보보호위원회 출연금으로 수행한  
사업의 결과물입니다.

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.12

## PRiVACY REPOR[T

