

## EXECUTIVE BRIEFING

# AI 시대, 글로벌 기업의 개인정보 거버넌스 및 대응 전략

작성자: Privacy Managing Counsel

수신: 경영진(CEO, CAO, CISO, CLO), 법무·컴플라이언스·데이터 보안 책임자

목적: AI 확산 및 글로벌 규제 강화에 따른 데이터 법적 리스크 관리 및 대응 체계 수립

## Executive Summary

AI 기술의 비약적인 발전과 글로벌 확산은 기업에게 전례 없는 사업적 기회를 제공하는 동시에, 데이터 규제 준수(Data Compliance) 측면에서 치명적인 리스크를 동반하고 있습니다. 과거의 개인정보 관리가 단순한 '약관 동의' 및 '내부 보안 점검'에 머물렀다면, 현재는 **글로벌 사업 존속 여부를 결정짓는 핵심 규제 리스크 관리 영역**으로 진화했습니다.

본 보고서는 글로벌 개인정보 규제 트렌드를 파악하고, 최근 대규모 제재 사례의 시사점을 분석하여, AI 시대에 CAO 및 C-Level 경영진이 반드시 구축해야 할 **글로벌 개인정보 핸들링 프레임워크**를 제시합니다.

## SESSION 1. 개인정보 법령 위반과 규제 사례 분석 (feat. 쿠팡, Meta)

최근 규제 당국의 집행 경향은 단순 행정지도 수준을 넘어 **기업 매출액에 비례하는 천문학적인 과징금 부과 및 형사 처벌, 서비스 중지 권고** 등 강력한 실력 행사로 전환되었습니다.

### 1. Meta (유럽연합 GDPR 및 타겟 광고 이슈)

- **사건 개요:** Meta는 사용자 행동 데이터를 기반으로 한 타겟 광고 제공 시, 이용자의 명시적 동의 대신 '계약 이행의 필요성'을 합법적 근거로 주장하였으나 유럽 데이터보호위원회(EDPB) 및 규제 당국으로부터 거부당함.
- **시사점 및 리스크:**
  - **합법적 처리 근거의 엄격성:** AI 기반 추천 알고리즘이나 타겟 마케팅 활용 시, 다호화된 동의 수집 및 법적 근거(Consent, Legitimate Interest 등)의 타당성을 정교하게 입증해야 합니다.
  - **초국가적 규제 연대:** EDPB를 필두로 한 유럽 당국의 일관된 대규모 제재 조치는 글로벌 플랫폼 사업 구조 전체를 재검토하게 만들고 있습니다.

### 2. 쿠팡 (국내 개인정보보호법 및 데이터 안전성 확보 조치)

- **사건 개요:** 대규모 고객 데이터 유출 및 내부 접근 통제 미비, 위탁/재위탁 과정에서의 관리·감독 소홀 등으로 인한 감독당국의 조사 및 제재.

- 시사점 및 리스크:

- **내부자 리스크 및 접근 권한 관리(IAM):** AI 시스템 학습용 데이터 인프라 구축 시, 내부 임직원 및 외부 협력사의 접근 권한을 최소화(Least Privilege)하지 않을 경우 치명적인 침해 사고로 이어집니다.
- **유출 사고 발생 시 2차 파급력:** 단순 과징금에 그치지 않고 브랜드 신뢰도 하락, 집단 소송, 경영진 징계 등 비즈니스 연속성(Business Continuity)에 심각한 타격을 입게 됩니다.

## SESSION 2. 글로벌 개인정보 관련 법령의 구조 및 동향

글로벌 시장 진출 기업이 파편화된 규제 환경(Regulatory Fragmentation)에 대응하기 위해서는 각 권역별 핵심 법령의 구조를 명확히 이해해야 합니다.

### Global Privacy & AI Regulatory Landscape



### 1. EU (GDPR & EU AI Act)

- **GDPR (일반개인정보보호법):** 글로벌 데이터 보호 기준의 표준. 역외 적용(Extra-territorial effect) 규정에 따라 EU 거주자의 데이터를 처리하는 모든 글로벌 기업에 적용.
- **EU AI Act (인공지능법):** 세계 최초의 종합 AI 규제법. AI 시스템의 위험도(Unacceptable, High, Limited, Minimal Risk)에 따른 차등적 의무 부과. 고위험 AI의 경우 데이터 품질 관리, 기술 문서화, Human Oversight(사람의 개입)가 의무화됨.

### 2. 미국 (State-level Privacy Laws)

- 연방법 차원의 종합 개인정보보호법의 부재 속에서, **캘리포니아(CCPA/CPRA)**를 시작으로 버지니아, 콜로라도 등 각 주별로 독자적인 개인정보보호법 시행 중.
- **특징:** 소비자에게 데이터 판매/공유 거부권(Opt-out), AI 기반 자동화된 의사결정(Automated Decision-Making)에 대한 거부권 보장 강화.

### 3. 한국 (개인정보보호법 - PIPA)

- 개정 개인정보보호법 시행으로 **전체 매출액의 최대 3%**에 달하는 과징금 부과 가능.
- **자동화된 의사결정에 대한 권리:** AI 등을 통한 자동화된 평가·결정에 대해 거부하거나 설명을 요구할 수 있는 권리가 신설되어 AI 모델 운용 시 설명가능성(XAI) 확보 필요.

### 4. 역외 데이터 이전 (Cross-Border Data Transfer)

- 국가 간 데이터 이동 시 **적정성 결정(Adequacy Decision)**, **표준계약조항(SCCs)**, **기업결합규칙(BCR)** 등 적합한 데이터 이전 메커니즘 수립 필수.

## SESSION 3. AI 시대, 글로벌 개인정보 핸들링 전략

---

AI 모델의 개발(Training), 검증(Validation), 서비스 제공(Inference) 등 전 주기(Lifecycle)에 걸쳐 법적 리스크를 격리(Isolate)하기 위한 4단계 대응 전략을 제안합니다.

### 1. AI 데이터 수집 및 학습 단계의 합법성 확보

- **데이터 출처(Data Provenance) 검증:** 웹 스크래핑, 제3자 데이터 매입 시 저작권 및 개인정보 수집·이용 동의 범위의 합법성 점검.
- **가명정보 및 익명정보 활용:** 학습 데이터 구축 시 개인을 식별할 수 없도록 가명화(Pseudonymization) 또는 익명화(Anonymization) 처리 프레임워크 적용.

### 2. Privacy by Design & Default (초기 단계부터의 개인정보 보호)

- AI 제품/서비스 기획 단계부터 개인정보 영향평가(PIA) 및 AI 리스크 평가를 수행.
- **데이터 최소화 원칙(Data Minimization):** AI 모델 성능 향상에 반드시 필요한 데이터만 최소한으로 수집·활용.

### 3. AI Governance & Transparency (투명성 및 설명가능성)

- **이용자 고지 체계 확립:** 생성형 AI 서비스 제공 시 AI에 의해 생성된 콘텐츠를 명시하고, 사용자 입력 데이터가 모델 재학습(Re-training)에 활용되는지 여부를 선택(Opt-in / Opt-out)할 수 있도록 조치.
- **옵트아웃(Opt-out) 및 삭제(Unlearning) 메커니즘:** 이용자의 데이터 삭제 요청 시, 이미 학습된 AI 모델에서 특정 개인의 데이터를 분리 또는 제거할 수 있는 기술적/관리적 대안 수립.

### 4. 이사회, C-Level(CAIO 등) 중심의 통합 거버넌스 구축

- 법무, 보안, AI 엔지니어링, 사업 부서가 참여하고 **CAIO가 공동 주도하는 'AI Privacy Committee(가칭)'** 신설.
- 전사 차원의 AI 데이터 활용 가이드라인(AI Code of Conduct) 수립 및 수시 감사(Audit) 체계 운영.

## 결언 및 C-Level / CAIO Action Items

---

AI 시대의 개인정보 관리 및 컴플라이언스는 단순히 법적 처벌을 피하기 위한 **비용(Cost)**이 아닌, 글로벌 시장에서 고객의 신뢰를 확보하고 기업 가치를 제고하는 **경쟁력(Competitive Advantage)**입니다.

### 경영진 및 CAIO를 위한 3가지 즉시 실행 과제

1. **전사 AI 데이터 데이터 맵(Data Map) 작성:** 현재 구축·운용 중인 AI 모델 및 데이터 흐름에 대한 전수 조사를 CAIO 및 CISO 주도로 실시.
2. **글로벌 규제 갭 분석(Gap Analysis):** 목표 진출국(EU, 미국 등)의 데이터/AI 규제 대비 자사 시스템의 미비점 파악.
3. **AI 이머전시 대응 프로세스 구축:** 데이터 유출 또는 AI 편향성/오남용 사고 발생 시 즉시 가동할 위기 관리 온콜(On-call) 체계 가동.