국제법무지원
NEWS LETTER

2025 JUN

해외규제 모니터링 제8호

최신 데이터 및 개인정보 규범 동향

"본 뉴스레터는 법무부 국제법무지원과 '규제 리포트'와 前 개인정보위 부위원장을 역임하신 성균관대 인공지능융합원 최영진 교수님의 칼럼으로 구성되어 있습니다."

규제 리포트

최신 데이터 및 개인정보 규범 동향 리포트
- 유럽·미국·중국·일본 등 주요 국가들의 제정 규범을 중심으로 -

법무부 국제법무지원과

▣ 디지털화와 AI 시대 도래에 따른 데이터 규범 제정

■ 2020년대 중반에 접어들며 세계 각국은 디지털 주권 강화와 개인정보 자기결정권 보장을 중심으로 개인정보 보호 관련 입법 및 제도 정비를 가속화하고 있습니다.

■ EU는 「일반개인정보보호법(General Data Protection Regulation, GDPR)」을 기반으로 개인정보의 통제와 데이터 이동에 대한 기준을 정립하고 있으며, 미국은 부문별·주별 규제에서 연방 단위 입법 논의로 전환되는 양상으로 접어들고 있습니다.

■ 한편, 중국은 데이터 통제를 국가안보와 직접 연결하여 외국계 기업에 대한 관리·감독 기준을 수립하였으며, 일본은 유럽과의 제도 정합성을 강화하는 방향으로 법 개정을 지속 중입니다.

■ 이에 본 리포트는 주요 국가의 개인정보 보호 규제체계 현황을 검토하고, 우리 기업에 미치는 영향을 중심으로 시사점을 도출하고자 합니다.

▣ 유럽연합(EU) : GDPR 시행을 통한 개인정보 전면 규제

"강력한 개인정보 보호는 혁신의 장애물이 아니라 디지털 시대에서 신뢰의 전제조건입니다."

– Dider Reynders, EU 집행위원회 법무위원장, '22. 1. 기자회견 中 –

■ 유럽연합(EU)은 '16년 「일반개인정보보호법(General Data Protection Regulation, GDPR)」을 채택 후, '18년 5월 25일부터 정식 시행하여 EU 역내·역외 기업에 광범위한 개인정보 보호의무를 부과하고 있습니다.

■ GDPR의 주요 내용으로는 ▲명확한 동의 원칙, ▲정보주체 권리 강화(열람권·정정권·삭제권·이동권 등), ▲처리 책임성 원칙(accountability), ▲DPO(Data Protection Officer) 지정 의무, ▲개인정보 유출 시 72시간 내 통지의무 등이 있습니다.

■ GDPR은 역외효(effect of extraterritoriality)를 갖는바, EU 시민의 개인정보를 처리하는 역외 기업에도 동일하게 적용됩니다.

【GDPR 위반 사유별 과징금 정리】

구 분	개 요
연간 전세계 매출액의 2% 또는 1천만 유로 중 더 큰 금액	– 개인정보처리자의 기록 유지 의무 불이행 – DPO 지정의무 위반 – 보안조치 미흡 – 개인정보 유출에 대한 통지의무 불이행 – 개인정보처리 위탁계약의 형식적 요건 위반
연간 전세계 매출액의 4% 또는 2천만 유로 중 더 큰 금액	– 개인정보 처리의 기본 원칙 위반(적법성, 목적제한성, 최소성 등) – 정보주체 권리 침해(열람권, 정정권, 삭제권 등) – 역외이전 요건 미준수 – 감독기관 명령 불이행

■ 최근에는 AI 시대 도래에 따른 「AI법(AI Act)」과의 연계 가능성, GDPR의 해석을 둘러싼 유럽사법재판소(CJEU) 판례 등으로 관련 법령의 적용 범위가 더욱 확대되는 추세입니다.

■ 예를 들어, Fashion ID 판결(ECJ, C-40/17)은 GDPR 제26조에 규정된 개인정보 처리의 공동 통제자(joint controller) 개념을 확장하고 제3자 플러그인 사용 시의 책임 분배 등 법적 고려사항을 재확인하였다고 평가됩니다.

- 위 판결에서 온라인 의류소매업체 Fashion ID는 자사 웹사이트에 소셜 네트워크 서비스인 Facebook Ireland(이하 '페이스북')의 소셜 플러그인 중 하나인 '좋아요 버튼'을 설치하였고, 페이스북은 위 플러그인을 통해 Fashion ID 웹사이트에 방문한 이용자의 개인정보를 수집하였습니다.
- 위 판결에 따르면, 복수의 주체가 개인정보 처리의 목적과 수단을 결정하는 경우 「공동 통제자」가 되어 개인정보 보호에 대한 책임을 부담하게 되며, 각 개인정보 처리 단계별로 통제자 해당 여부에 대한 판단은 달라질 수 있습니다.

▣ 미국 : 주별 법령 중심의 분산형 규제체계

"미국 국민은 현대 디지털 도구 사용을 위해 프라이버시를 희생해서는 안 됩니다. FTC는 개인정보를 오용하는 기업에 책임을 묻겠습니다."

– FTC 위원장 Lina Khan, '23. 11.자 연례 프라이버시 포럼 발언 中 –

■ 미국은 연방 차원의 포괄적 개인정보보호법보다는 주(州)별 입법에 의존하여 소비자 프라이버시를 보호하고 있습니다.

■ 대표적인 법률은 2018년 캘리포니아주가 제정한 「캘리포니아 소비자 프라이버시법(California Consumer Privacy Act, CCPA)」이며, 이는 2023년에 「캘리포니아 프라이버시권리법(California Privacy Rights Act, CPRA)」으로 개정되어 현재까지 시행되고 있습니다.

• CPRA는 ▲소비자의 정보 접근·삭제·이의제기권, ▲민감정보 보호, ▲자동화된 의사결정 대응권, ▲프라이버시 전담 감독기구 설치 등을 포함하고 있습니다.

■ 2022년 CPRA의 전신인 CCPA의 최초 위반 사례로 미국 화장품 기업 세포라(Sephora)가 조정을 거쳐 약 120만 달러 과징금 납부에 합의한 사례가 있습니다.

• 세포라(Sephora)가 자사 웹사이트 방문자의 개인정보를 제3자 광고업체에 공유한 점, 그 사실을 소비자에게 고지하지 않은 점 및 'Do not sell my personal information' 버튼을 올바른 방식으로 제공하지 않은 점이 문제가 된 사례였습니다.

■ 현재까지 버지니아, 콜로라도, 유타, 코네티컷주 등도 자체적인 개인정보 보호법을 제정하여 시행 중이며, 연방 차원에서는 2022년 「American Data Privacy and Protection Act(ADPPA)」 초안 공개 후 입법 논의를 지속 중입니다.

【EU GDPR과 美 CPRA 비교】

구 분	주요 협력분야	프로그램에서의 역할
정보주체로부터 개인정보 수집·이용동의를 받는 방식	– 우선 개인정보를 처리하고, 정보주체가 사후에 거부의사를 표시할 경우, 그때 비로소 정보처리를 멈추는 옵트아웃(Opt-out) 방식 – 단, 16세 미만의 정보주체로부터 동의를 받는 경우 옵트인 방식	– 정보주체로부터 사전에 개인정보 처리 관련 동의를 받은 후 정보를 처리하는 옵트인(Opt-in) 방식
적용 대상	– 캘리포니아주에서 영업하는 기업 中 ① 연간 매출이 2,500만 달러 이상이거나, ② 100,000건 이상의 캘리포니아 주민 개인정보를 보유하거나, ③ 개인정보 판매 및 공유에 따른 매출이 기업의 총 매출의 50% 이상을 차지하는 기업	– EU 시민의 개인정보를 처리하는 모든 기업, 기관 및 개인
정보주체의 권리	– 열람권, 정정권, 삭제권 등 보장	– 열람권, 정정권, 삭제권 등 뿐만 아니라 이의제기권, 처리제한권, 동의철회권 등 더 폭넓은 권리를 정보주체에게 보장

▣ 중국 : 전면적 데이터 통제 및 국가안보 중심의 규제 강화

■ 중국은 2021년 중화인민공화국개인신식보호법(中华人民共和国个人信息保护法)과 중화인민공화국데이터안전법(中华人民共和国数据安全法)을 연이어 시행하며, 데이터 규제를 국가안보 및 공공질서 보호 관점에서 강화하고 있습니다.

■ 「중화인민공화국개인신식보호법」은 ▲개인정보 처리에 대한 명확한 동의 요구, ▲처리 목적 제한, ▲역외 이전 시 보안성 심사 등 GDPR과 유사한 구조를 취하고 있습니다.

■ 「중화인민공화국개인신식보호법」에 따를 때, 개인정보처리자가 중국 내 데이터를 역외 이전 하려면 아래와 같은 절차를 거쳐야 합니다.

- 먼저 개인정보처리자는 정보주체로부터 역외 이전에 관한 명확한 동의를 얻고 개인정보영향평가보고서를 작성하여야 합니다.
- 다음으로, 개인정보처리자는 ①국가인터넷정보판공실(国家互联网信息办公室)의 표준계약 체결, ②보안성 평가, ③국가가 지정한 인증기관의 인증 중 하나 이상의 요건을 충족해야 합니다.

■ 한편,「중화인민공화국데이터안전법」은 ▲중요데이터의 분류 및 등급별 관리, ▲데이터거래 규제, ▲정부의 실시간 접근권 등을 규정합니다.

▣ 일본 : 개인정보보호법 개정을 통한 역외이전 및 AI 대응 강화

■ 일본은 '03년 「개인정보의 보호에 관한 법률(個人情報の保護に関する法律)」을 제정 후, '17년, '20년, '22년 등 지속적인 개정을 통해 자국 법률이 개인정보 보호 관련 국제기준에 부합하도록 조정하여 왔습니다.

- 위 법률은 ▲익명가공정보 제도 도입, ▲정보주체의 동의 원칙, ▲개인정보 제3자 제공 시 기록 보존, ▲개인정보처리사업자의 관리책임 강화 등을 규정하고 있습니다.
- 특히 '22년 개정에서는 ▲역외이전 요건 명확화, ▲거버넌스 강화, ▲법 위반 시 과징금 상향(관련매출의 최대 5%) 등 GDPR과 유사한 구조로 개편하였습니다.

■ 일본은 '19년 EU와의 상호적정성 결정(mutual adequacy)을 통해 개인정보의 자유로운 양방향 이동이 가능하게 되었으며, 최근에는 'AI 윤리 가이드라인', '데이터 이동 활성화 전략' 등을 통해 데이터 경제 기반을 구축하고 있습니다.

▣ 결론

■ 주요국의 개인정보 보호 법제는 각국의 정치·경제·안보적 특성을 반영하여 상이하게 발전하고 있습니다.

■ 우리나라도 '23년 6월 「제5차 개인정보 보호 기본계획(2024~2026)」을 수립하여 "디지털 신뢰 사회 실현"이라는 비전을 제시하고, 이에 따라 '24년 「AI 개인정보 보호 가이드라인」을 마련하는 등 개인정보 보호를 위한 정책 기반을 정비하고 있습니다.

• 또한, 2011년 제정된 우리 개인정보 보호법은 제정 과정에서부터 EU GDPR의 전신인 Directive 95/46/EC를 주요 참고자료로 활용하였으며, 옵트인 방식을 채택하는 등 GDPR과 유사한 형태로 개인정보 보호에 대한 법적 규율을 강화하고 있습니다.

■ 이와 관련하여 ① 개인정보보호위원회 및 한국인터넷진흥원 편찬 '우리기업을 위한 2022 EU일반개인정보보호법 가이드북', ② 유럽연합 일반개인정보보호법(GDPR) 번역본, ③ 美 캘리포니아주 프라이버시권리법(CPRA) 원문을 본 게시물과 함께 별도로 첨부했습니다.

■ 법무부는 앞으로도 우리나라의 산업·경제에 상당한 영향을 미칠 주요 국가들의 최신 개인정보 관련 정책·법제 등을 적극 모니터링하고 외부 전문가들의 의견을 수렴하여, 해외 시장 진출을 희망하는 우리 기업의 경영활동에 도움이 되도록 노력하겠습니다.

담당자_ 국제법무지원과 사무관 **황현준**, 법무관 **이동건**