2024 Privacy Report

개인정보보호 월간동향분석

2월호

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2024 Privacy Report

개인정보보호 월간동향분석

2월호

1. 미국 주(州) 개인정보 보호법에 대한 평가 및 분석

2. DPO지정 및 역할에 대한 CEA 2023 조사 분석

KISA

미국 주(州) 개인정보 보호법에 대한 평가 및 분석

[목 차]

1. 개요

▶ **(개요)** 미국 전자개인정보센터(EPIC)[1]가 미국 PIRG교육펀드(U.S. PIRG Education Fund)[2]와 함께 발표한 미국 주(州)별 개인정보 보호법 제정 현황 분석 보고서에 따르면, 주법으로 마련된 개인정보 보호법 중 대다수가 실질적이고 의미있는 보호 조치를 제공하지 못하고 있는 것으로 평

- '24년 2월 1일까지 총 14개 주에서 포괄적인 개인정보 보호법이 통과되었으나, 이들 주 가운데 절반가량(6개 주)이 소비자 개인정보 보호법 평가에서 낙제 등급('F')을 받았고, 최고 등급('A')을 받은 주는 한 곳도 없는 것으로 확인

- 그나마 높은 평가를 받은 캘리포니아주('B+')를 제외한 다른 주들은 산업계의 강력한 로비 속에서 빅테크가 작성한 개인정보 보호법 초안을 기반으로 개인정보 보호법을 수립했고, 이것이 개인정보 보호 조치를 약화시킨 배경이 된 것으로 분석

1) Electronic Privacy Information Center: 개인정보 보호, 표현의 자유, 민주적 가치 등을 옹호하기 위해 설립된 비영리 연구센터
2) 소비자 보호를 위한 시민단체인 미국 공익 리서치 그룹(US PIRG)의 파트너 연구기관 중 하나

▶ **(개선 방향)** EPIC은 개인정보 보호 조치를 강화하기 위해 관련 법률에 포함되어야 할 조치들로 ▲데이터 최소화 의무화 ▲민감한 개인정보 사용 규제 ▲온라인에서의 인권 보호(차별 금지) ▲소비자 프로파일링 제한 ▲강력한 집행 및 규제 권한 등을 강조

2. 미국 주 개인정보 보호법 현황 및 분석

(1) 개인정보 보호법 도입 배경

▶ **(필요성)** 오늘날 거의 모든 온라인 상호작용은 개인에 대한 데이터를 생성하고 있으며, 기업들은 놀랍고 위험한 방식으로 개인정보를 다량으로 수집하여 활용 중

- 무분별한 개인정보 수집은 보안 위험을 키울 뿐만 아니라 스캠(scam), 신원도용과 같은 범죄 위험을 확대하고, 프로파일링 등으로 개인에 대한 차별을 초래
- 또한, 데이터 브로커에게 전송 또는 판매된 개인정보는 맞춤형 광고에 사용되거나, 종종 이자율 결정 알고리즘 등 개인에게 불리할 수 있는 의사결정에 활용됨

▶ **(도입 배경)** 소수의 빅테크들이 다량의 개인정보 수집 및 판매를 통해 수십억 달러를 창출하고 있음에도 불구하고, 미국 연방법에는 포괄적인 개인정보 보호법이 존재하지 않음

- 개인정보 처리 행위를 규율하는 기존의 연방 '프라이버시법(Privacy Act of 1974)' 은 시장 자율 규율(self-regulation) 방식을 따르고 있으며, 스마트폰 및 인터넷이 보편화된 최근의 상황을 적절히 반영하지 못함
- 다만, 보건의료, 금융, 아동보호 등 여러 개별적인 영역에서 개인정보 보호 조항을 포함하는 연방법과 주법이 제정되어 시행 중*

  * 연방법의 대표적인 예로 의료정보에 대해 규제하는 '의료정보 보호법(Health Insurance Patient Privacy Act)', 금융기관에 적용되는 '금융현대화법(Gramm-Leach-Bliley Act)' 등이 있고, 주법의 예로는 '캘리포니아 의료정보 비밀유지법(California's Confidentiality of Medical Information Act)' 등이 존재

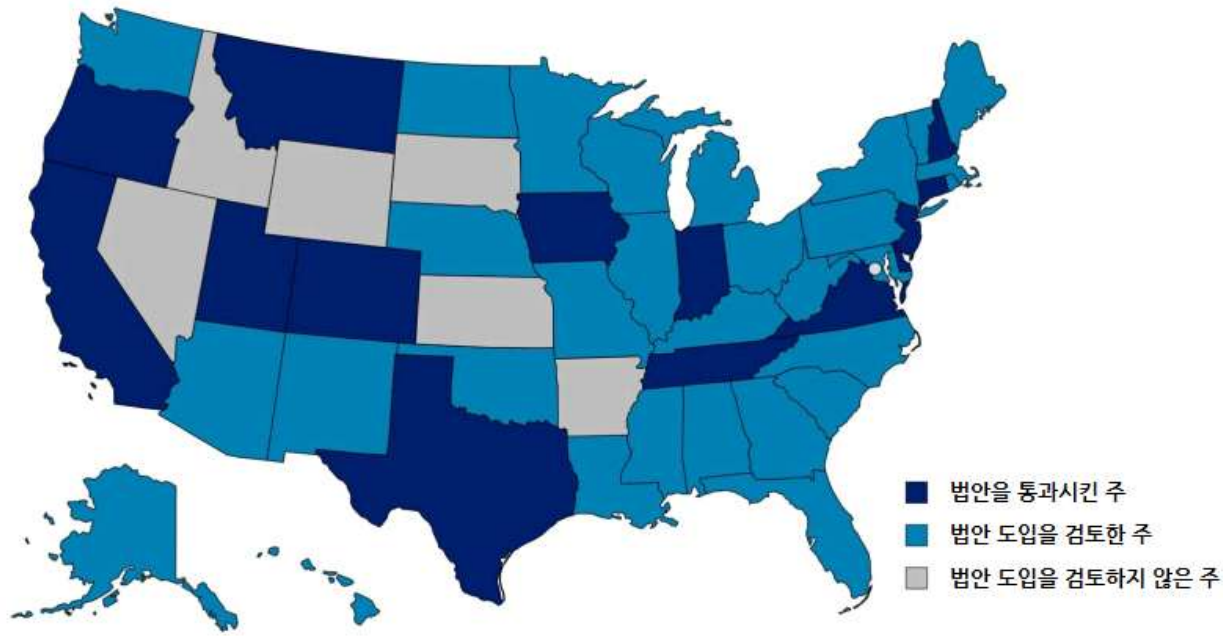
- 이 가운데 점점 더 많은 주들이 개인정보 보호 및 보안을 위한 별도의 포괄적인 개인정보 보호법을 추진

(2) 개인정보 보호법 추진 현황

▶ '18년 이후 미국에서는 44개 주가 개인정보 및 보안을 위한 법안 도입을 검토했고, '24년 2월 1일을 기준으로 총 14개 주에서 관련 법안을 통과시킴

- 그러나 EPIC의 평가 결과에 따르면, 14개 주에서 통과된 법안 중 대부분은 강제력이 미약하고 기업 친화적이므로, 기업들은 큰 제약 없이 계속해서 소비자 개인정보의 수집·축적·이용이 가능한 반면 소비자는 권리 행사가 어려운 실정

그림 _ 미국 주의 포괄적 개인정보 보호법(안) 추진 현황



출처: EPIC(2024)

(3) 14개 주 개인정보 보호법 평가 결과

▶ **(평가 대상)** EPIC은 개별 영역에 한정되지 않는 포괄적인 개인정보 보호법을 통과시킨 14개 주의 법(안)에 대한 평가를 실시

▶ **(평가 방법 및 기준)** 14개 주의 개인정보 보호법에 다음의 개인정보 보호 조치들이 적절하게 포함되었는지를 검토하여 점수를 부여

- **(데이터 최소화 조치)** 여러 데이터 최소화 조치*에 대한 조항의 존재 유무와 내용

  * ▲데이터의 수집·처리·전송을 개인이 요청한 제품 및 서비스 제공에 필요한 경우로 한정 ▲더 이상 필요 하지 않은 데이터 삭제 의무화 ▲유전자·생체·위치 정보 등 민감한 데이터의 수집 및 처리 제한 ▲기본적으로 데이터의 2차 처리 및 전송 금지(일부 예외만 허용) ▲제3자에게로의 민감한 데이터 전송 금지 및 옵트인(Opt-in) 동의가 있을 경우에만 허용 ▲여러 데이터 컨트롤러로부터 얻은 데이터의 2차 활용 및 결합 금지 등

- **(강력한 집행력)** 법 집행을 위해 주 법무장관에 강력한 권한을 부여하거나, 독립적인 개인정보 감독기관을 설립하거나, 개인정보 침해에 대해 개인이 기업에 소송을 제기할 수 있는 권한(개인 소송권)을 인정하는지 여부

- **(규칙제정 권한)** 개인정보 보호법 준수를 위한 지침을 제공하고, 동 법이 기술 변화에 부응할 수 있도록 관련 규칙을 제정할 수 있는 권한을 규정하고 있는지 여부

- **(민권 보호)** 인종, 피부색, 종교, 출신국가, 성별, 장애 등에 근거해 상품이나 서비스를 차별적으로 제공하기 위한 개인정보의 수집·처리·전송을 금지하는 조항의 유무

- **(투명성 및 고위험 개인정보 처리 관행에 대한 평가)** 개인정보 처리 관행에 대한 영향 평가* 및 문서화 관련 조항의 포함 유무와, 이러한 평가 내용에 대해 일반 대중의 접근을 허용하고 있는지 여부

  * 수집되는 개인정보의 유형, 목적, 사용 및 전송/판매 여부 및 방법, 개인정보의 수집 및 활용으로 인한 소비자의 잠재적 위험과 잠재적 혜택, 혜택이 위험보다 더 큰 이유, 위험을 완화할 수 있는 방법, 프로파일링에 대한 대안 및 이러한 대안을 활용하지 않는 이유 등에 대한 내용 등을 포함

- **(유의미한 개인의 권리)** 개인정보에 대하여 접근·수정·삭제 등을 요청할 수 있는 개인의 권리가 인정되고 있는지 여부*

  * 일반적인 옵트아웃(Opt-out) 신호에 대한 존중, 소비자 및 기타 관련 데이터에 대한 삭제권, 개인정보가 공개된 제3자에 대한 정보를 얻을 수 있는 권리, 승인된 대리인의 전적인 권리 행사 인정 등에 대한 내용 포함

- **(조작적 설계 및 불공정 마케팅 방지)** 불공정한 비즈니스 관행을 방지하는 조치*의 유무

  * ▲로열티 프로그램을 위해 수집된 데이터의 사용은 해당 프로그램을 운영하는 데에 기능적으로 필요한 정도로만 제한(제3자 판매 또는 맞춤형 광고에 활용 금지) ▲개인정보 보호 권리를 행사하는 소비자에 대한 차별적 취급 금지(맞춤형 광고를 거부한 소비자에게 더 높은 가격을 청구하는 행위 등을 금지) ▲소비자로부터 개인정보 활용 동의를 얻기 위한 다크패턴이나 조작적 설계 사용 금지 등

- **(강력한 용어 정의)** 개인정보, 데이터 컨트롤러/대상기업, 판매/공유/이전, 프로파일링, 맞춤형 광고, 생체정보 등 개인정보 보호에 있어 중요한 용어들을 엄격하게 정의하고 있는지 여부

표 1_ 중요 용어 정의 시 고려할 사항

- 개인정보: 개인이나 가정, 기기에 연결되어 있거나 연결될 수 있는 정보(추론 또는 파생된 정보 포함)로 정의되어야 하며, 가명정보라도 다른 정보와 함께 개인 식별에 활용될 수 있으므로 개인정보 보호법 적용을 면제하지 않아야 함
- 컨트롤러/대상기업: 개인정보 보호법의 적용 범위는 회사의 수익이 아닌 해당 회사가 처리하는 데이터의 양을 기준으로 해야 함
- 판매/공유/이전: 금전적인 가치만이 아니라 모든 상업적인 목적을 고려하여 개인정보 판매에 대해 정의하여야 함
- 프로파일링: 프로파일링 또는 자동화된 의사결정 시스템에 대한 정의는 해당 시스템의 기능 즉, 인간의 의사결정을 지원하거나 대체하는 것에 초점을 맞춰야 하며 정교한 AI모델뿐만 아니라 단순한 알고리즘이나 자동화 프로세스 모두를 아울러야 함
- 맞춤형 광고: 맞춤형 광고에 대한 정의는 소비자의 기대와 일치해야 함
- 생체정보: 개인 식별을 목적으로 활용하는 정보뿐만 아니라 개인을 식별할 수 있게 해주는 고유의 정보로 폭넓게 정의되어야 하며, 지문이나 얼굴인식 정보는 개인 식별을 위해 사용되는지 여부에 관계없이 매우 민감한 개인정보로 간주

▶ **(평가 결과 및 분석)** 14개 주 가운데 캘리포니아 주가 가장 높은 점수를 획득했고, 버지니아주를 비롯한 6개 주는 낙제 등급을 받음

- 캘리포니아 주는 '18년 미국 주 가운데 최초로 포괄적인 소비자 개인정보 보호법을 통과시켰고, 동 법은 전반적으로 소비자 개인정보 보호에 대한 실질적인 보호 조치를 확립한 것으로 평가
- 그러나 14개 주 모두에서 데이터 최소화와 개인 소송권에 대한 조항은 불충분하거나 부재한 것으로 평가
- 낙제 등급을 받은 6개 주 가운데 먼저 포괄적인 개인정보 보호법을 채택한 버지니아주에서는 아마존이 로비스트를 통해 주 상원의원에게 전달한 법안초안이 '21년 주법으로 제정
- 낙제 등급을 받은 나머지 주들은 이러한 '버지니아 주 모델'을 채택했고, 그 결과 이들 주에서도 버지니아주와 유사한 기업 친화적인 개인정보 보호법이 마련됨

표 2_ 미국 14개 주의 개인정보 보호법 평가 결과 요약

주 (등급, 점수)	개인정보 보호법	법률에 포함된 주요 개인정보 보호 조치	누락된 개인정보 보호 조치	개선 방향 (권고사항)
캘리포니아 (B+, 69점)	California Consumer Privacy Act (2020.1.1. 발효)	• 독립적인 개인정보 감독기관[3] 설립 • 불공정한 금융 인센티브 제공 금지 • 다른 개인정보 보호 관련 법률에서 규율하는 개인정보 처리에 대해 적용을 면제하되, 면제 범위를 규제대상(기업)이 아닌 개인정보로 제한[4] • 가명정보에 대한 예외 불인정 • 개인정보 보호를 약화시키는 법개정 금지[5]	• 민감한 개인정보에 대한 보다 강력한 보호 조치 부재 • 사이트 간 브라우저 추적에 대한 명확한 제약사항 부재 • 데이터 최소화 프레임워크에 세부적인 제한사항 부재 • 데이터 침해로 귀결되지 않은 법률 위반에 대한 개인 소송권 관련 내용 부재	• 생체정보에 대한 보다 엄격한 정의 수립 • 실효적인 민권 보호가 가능하도록 차별 금지 조항 강화 • 규칙제정 권한을 계속 활용하여 소비자 개인정보 및 권리 보호

4) 예를 들어, 연방 금융현대화법은 동 법의 규제 대상인 금융기관들의 개인정보 처리와 관련한 조항을 포함하고 있는데, 캘리포니아 주의 개인정보 보호법은 동 법의 적용을 받는 금융기관들의 개인정보 처리에 대해서는 개인정보 보호법의 적용을 면제하지만 해당 금융기관 자체에 대한 법 적용을 면제하지는 않음. 따라서 소비자는 데이터 침해 사건 발생 시 금융기관에 대해서도 개인정보 보호법에 따른 소송 제기가 가능

5) 원칙적으로 주의회에서 과반 이상이 찬성하는 경우 법 개정이 가능하나, 캘리포니아 주의 개인정보 보호법은 오직 개인정보 보호를 더욱 강화할 수 있는 방향으로만 법 개정이 가능하도록 허용하고 개인정보 보호를 약화시키는 법 개정은 불가하도록 함(되돌리거나 후퇴할 수 없다는 의미에서 '역진방지(One-Way Ratchet)' 원칙으로 알려짐)

6) 의무불이행 사항에 대하여 일정 기간 내에 보완이 가능하도록 허용

주 (등급, 점수)	개인정보 보호법	법률에 포함된 주요 개인정보 보호 조치	누락된 개인정보 보호 조치	개선 방향 (권고사항)
콜로라도 (C+, 41)	Colorado Privacy Act (2023.7.1. 발효)	• 주 법무장관에 규칙 제정 권한 부여 • 데이터 컨트롤러에 일반적인 옵트아웃 신호에 대한 존중 요구 • 다른 개인정보 보호 관련 법률에서 규율하는 개인정보에 대해서만 제한적으로 적용 면제 • 다크패턴/눈속임 설계 금지	• 개인 소송권 인정 조항 부재 • 불충분한 데이터 최소화 요건	• 개인정보 판매/공유에 대한 보다 엄격한 정의 수립 • 차별 금지 조항 강화 • 기업에 영향평가 결과(또는 요약본)에 대한 일반 공개 요구 • 개인정보 보호 권리를 행사한 소비자에 대한 가격 차별 금지 • 규칙제정 권한을 계속 활용하여 소비자 개인정보 및 권리 보호
뉴저지 (C, 37)	Senate Bill 332 (명칭 미정, 2025.1.16. 발효 예정)	• 주 법무장관에 규칙제정 권한 부여 • 가명정보에 대한 예외 불인정	• 데이터 최소화 요건 부재 • 개인 소송권 인정 조항 부재	• 차별 금지 조항 강화 • 기업에 영향평가 결과(또는 요약본)에 대한 일반 공개 요구 • 개인정보와 생체정보에 대한 보다 엄격한 정의 수립 • 연방 금융법의 적용을 받는 금융기관이 아닌, 해당 기관이 다루는 개인정보에 대해서만 제한적으로 면제 적용 • 규칙제정 권한을 최대한 활용하여 소비자 개인정보 및 권리 보호

주 (등급, 점수)	개인정보 보호법	법률에 포함된 주요 개인정보 보호 조치	누락된 개인정보 보호 조치	개선 방향 (권고사항)
오레곤 (C-, 31)	Oregon Consumer Privacy Act (2024.7.1. 발효 예정)	• 가명정보에 대한 예외 불인정 • 다른 개인정보 보호 관련 법률에서 규율하는 개인정보에 대해서만 제한적으로 적용 면제 • 민감한 개인정보를 "트랜스젠더 또는 제3의 성" 등을 포함하여 폭넓게 정의 • 소비자에게 자신 및 일반의 개인 정보가 공개된 제3자에 대한 목록을 얻을 수 있는 권리 부여	• 주 법무장관의 규칙제정 권한 부재 • 개인 소송권 인정 조항 부재 • 데이터 최소화 요건 부재	• 개인정보 판매/공유에 대한 보다 엄격한 정의 수립 • 차별 금지 조항 강화 • 기업에 영향평가 결과(또는 요약본)에 대한 일반 공개 요구
델라웨어 (C-, 30)	Delaware Personal Data Privacy Act (2025.1.1. 발효 예정)	• 18세 미만 미성년자 대상 맞춤형 광고 금지 • 민감한 개인정보를 폭넓게 정의 • 소비자에게 자신의 개인정보가 공개된 제3자에 대한 목록을 얻을 수 있는 권리 부여	• 주 법무장관의 규칙제정 권한 부재 • 개인 소송권 인정 조항 부재 • 데이터 최소화 요건 부재	• 개인정보, 판매/공유, 생체정보에 대한 보다 엄격한 정의 수립 • 연방 금융법의 적용을 받는 금융기관이 아닌, 해당 기관이 다루는 개인정보에 대해서만 제한적으로 면제 적용 • 차별 금지 조항 강화 • 기업에 영향평가 결과(또는 요약본)에 대한 일반 공개 요구
코네티컷 (D, 24)	Connecticut Data Privacy Act (2023.7.1. 발효)	• 데이터 컨트롤러에 일반적인 옵트아웃 신호에 대한 존중 요구 • 18세 미만 미성년자대상 맞춤형 광고 금지	• 주 법무장관의 규칙제정 권한 부재 • 개인 소송권 인정 조항 부재 • 데이터 최소화 요건 부재	• 개인정보, 판매/공유, 생체정보에 대한 보다 엄격한 정의 수립 • 차별 금지 조항 강화 • 기존 개인정보 보호 관련 법률에서 규율하는 기업이 아니라, 개인 정보에 대해서만 면제 적용

주 (등급, 점수)	개인정보 보호법	법률에 포함된 주요 개인정보 보호 조치	누락된 개인정보 보호 조치	개선 방향 (권고사항)
뉴햄프셔 (D, 22)	Senate Bill 255 (명칭 미정, 2025.1.1. 발효 예정)	• 주 법무장관에 일부 규칙제정 권한 부여	• 데이터 최소화 요건 부재 • 개인 소송권 인정 조항 부재	• 개인정보, 판매/공유, 생체정보에 대한 보다 엄격한 정의 수립 • 차별 금지 조항 강화 • 기업에 영향평가 결과(또는 요약본)에 대한 일반 공개 요구 • 기존 개인정보 보호 관련 법률에서 규율하는 기업이 아니라, 개인 정보에 대해서만 면제 적용 • 주 법무장관의 규칙제정 권한 확대
몬타나 (D, 20)	Consumer Data Privacy Act (2024.10.1. 발효 예정)	• 데이터 컨트롤러에 일반적인 옵트아웃 신호에 대한 존중 요구 • 동 법 발효 후 18개월 동안 법 집행에 대한 보완권[6] 인정	• 데이터 최소화 요건 부재 • 개인 소송권 인정 조항 부재 • 주 법무장관의 규칙제정 권한 부재	• 개인정보, 판매/공유, 생체정보에 대한 보다 엄격한 정의 수립 • 기존 개인정보 보호 관련 법률에서 규율하는 기업이 아니라, 개인정보에 대해서만 면제 적용 • 차별 금지 조항 강화 • 기업에 영향평가 결과(또는 요약본)에 대한 일반 공개 요구

낙제 등급(총점 20점 미만)	
주 (등급, 점수)	**개인정보 보호법**
텍사스 (F, 16)	Texas Data Privacy and Security Act (2024.7.1. 발효 예정)
인디애나 (F, 11)	Consumer Data Protection Act (2026.1.1. 발효 예정)
버지니아 (F, 11)	Consumer Data Protection Act (2023.1.1. 발효)
유타 (F, 6)	Utah Consumer Privacy Act (2023.12.31. 발효)
테네시 (F, 6)	Tennessee Information Protection Act (2025.7.1. 발효 예정)
아이오와 (F, 4)	Iowa Data Privacy Act (2025.1.1. 발효 예정)

출처: EPIC(2024), 넥스텔리전스(주) 재구성

4. 결론 및 시사점

▶ 현재까지 미국 14개 주에서 제정된 개인정보 보호법들은 모두 개인정보 보호 및 보안을 위한 실효적인 보호 조치를 완전히 확립하지 못한 것으로 평가

- 대다수의 주에서 특히 데이터 최소화, 개인 소송권, 주 법무장관의 규칙제정 권한 등과 관련하여 개인정보 보호 조치가 미비한 것으로 분석
- 비교적 양호한 평가를 받은 캘리포니아 주의 법률도 적용 대상기업에 구체적인 데이터 최소화 조치를 요구하거나 개인 소송권을 폭넓게 보장하지 못함

▶ 다수의 주가 규제 대상인 빅테크가 작성한 법안 초안을 모델로 입법을 추진했고 그 결과 강력한 개인정보 보호법 제정에 실패

- 산업계는 주의회에 대한 활발한 로비활동을 통해 기업에 불리할 수 있는 개인정보 보호법(안) 추진을 막았고, 이러한 현상은 연방 의회에서도 동일하게 포착
- EPIC은 많은 주에서 산업계가 선호하는 개인정보 보호법이 통과되고 있는 상황이 주민들에게 위협이 될 뿐만 아니라, 미래에 제정될 연방 수준의 개인정보 보호법에 대한 기준을 낮추는 잠재적 위험이 될 수 있다고 지적

▶ EPIC의 보고서는 미국 주들의 개인정보 보호법 제정 현황을 개괄하는 한편, 그 내용을 여러 세부 항목에 따라 평가함으로써 보다 강력한 개인정보 보호법을 마련하기 위해 필요한 조치들을 제시

- 데이터 최소화 조치 등 주의 개인정보 보호 수준을 진단하기 위해 세분화·체계화한 항목들은 평가 기준으로 활용되는 동시에 향후 개선이 필요한 부분들을 명확화 하는 데에 기여

Reference

1. Electronic Privacy Information Center(EPIC), The State of Privacy, 2024.2.
2. Biometric Update, Privacy group says data protections by US states differ greatly, 2024.2.8.
3. Consumer Watchdog, How Consumers Lose If California's Landmark Privacy Law is Preempted, 2022.8.17.
4. Californians for Consumer Privacy, Californians for Consumer Privacy Announce Opposition to ADPPA, 2022.8.10.
5. Dechert Ready Set Go: California Privacy Protection Agency Previews Draft Regulations, 2022.6.7.
6. Ballard Spahr, Connecticut poised To become fifth state to enact privacy law, 2022.5.4.
7. Skadden, California Consumer Privacy Act: A Compliance Guide, 2019.3.

DPO 지정 및 역할에 대한 CEA 2023 조사 분석

[목 차]

1. 개요

▶ **(개요)** '24년 1월 16일, EU 개인정보보호이사회(EDPB)가 DPO(Data Protection Officer)의 지정과 역할에 초점을 두고 참여한 조정집행조치(Coordinated Enforcement Action, 이하 CEA) 결과보고서*를 발표

* 2023 Coordinated Enforcement Action: Designation and Position of Data Protection Officers (Adopted on 16 January 2024)

- 동 조사에는 유럽 개인정보보호감독관(EDPS)[7]를 비롯해 유럽경제지역(EEA)의 25개 개인정보 감독기관(supervisory authority, 이하 SA)이 참여했으며, GDPR 시행이 5년 지난 시점에서 DPO가 직면한 문제를 평가하여 통찰력을 제공하는 것을 목표로 함

▶ **(CEF 도입 배경)** '20년 10월, EDPB는 '2021-2023 전략(EDPB Strategy 2021-2023)'의 두 번째 핵심축* 구현을 위해 조정집행 프레임워크(Coordinated Enforcement Framework, 이하 CEF)를 수립

* Pillar 2: Supporting effective enforcement and efficient cooperation between national supervisory authorities

- CEF의 운영 취지는 SA 간의 효과적인 법 집행 및 효율적인 협력 지원을 목표로 하며, 공통의 방법론을 통한 집행 조치 조율을 촉진하고자 함

- CEA는 CEF 추진을 위한 조치로, EDPB가 주제를 선정하면, CEF에 참여하는 SA들이 해당 주제에 대해 한 해 동안 국가 차원에서 조사를 진행 후 조사 결과를 취합·분석하여 후속 조치가 필요한지를 결정하는 방식으로 운영

- 제1차 CEA 조사는 공공 기관의 클라우드 서비스 사용에 초점을 두고 '22년 2월 15일 착수 후 '22년 한 해 동안 진행되었으며, 이번 보고서는 '23년 3월 15일 착수 후 '23년 한 해간 진행한 제2차 CEA 조사의 결과물임

표 1_ 2022-2024 EDPB Coordinated Enforcement Action 비교

CEA	주제	취지	조사 현황	참여 SA 수*	보고서 유무
2022 (제1차)	공공 부문의 클라우드 서비스 사용	• 국가 및 EU 공공 부문에서 클라우드 기반 솔루션에 의존하는 제품 및 서비스의 GDPR 준수 촉진 • 심층 인사이트를 통한 EU 차원 후속 조치 마련 • 조율된 지침과 조치를 통해 선도적인 관행을 장려하여 적절한 개인정보 보호 보장	완료	22개	○

7) European Data Protection Supervisor:

2023 (제2차)	DPO의 지정 및 역할	• SA들의 집행 지원을 위해 DPO의 ▲프로필 ▲지위 ▲직무 인사이트 확보 • 조직 내 DPO에게 적용되는 요건에 대한 인식 제고 • DPO가 GDPR에서 규정한 역할을 수행하도록 보장 • 추가 지침 및 기타 형태의 지원에 대한 DPO 및 조직의 요구사항 평가	완료	25개	○
2024 (제3차)	컨트롤러의 정보주체 접근권 구현	• 추후 공개 예정	진행 중	31개	추후 발표 예정

출처: 넥스텔리전스(주)

▶ **(방법론)** DPO에 대한 '23년 CEA는 개별 SA가 컨트롤러, 프로세서 및/또는 DPO를 대상으로 맞춤형 설문지를 발송하는 형태로 진행

- 이 중 ▲16개 SA는 컨트롤러 또는 프로세서에게 직접 연락을 취했으며 ▲7개 SA는 DPO에게 연락하고 ▲2개의 SA는 앞의 두 방법을 모두 활용하는 방식으로 설문조사를 진행
- 해당 설문지는 총 6만 1,962명에게 발송되었으며, 이 중 1만 7,490명이 설문에 응답

2. GDPR에 근거한 DPO 지정 의무 및 역할

▶ **(지정의무)** GDPR 제43조에 따라 모든 EU 기관 및 단체는 DPO를 임명할 의무가 있으며, GDPR 제37조는 다음 요건에 해당하는 컨트롤러 및 프로세서에게 DPO 지정 의무를 부과

- 법원을 제외한 공공기관 또는 단체에서 개인정보 처리를 수행하는 경우
- 컨트롤러 또는 프로세서의 핵심 활동이 정보주체에 대해 대규모로 정기적이고 체계적인 모니터링을 요구하는 경우
- 컨트롤러 또는 프로세서의 핵심 활동이 민감정보(GDPR 제9조) 및 형사상의 유죄 판결 및 범죄 행위 관련 개인정보(GDPR 제10조)의 대규모 처리를 동반하는 경우

▶ **(담당 업무)** GDPR이 규정한 DPO의 주요 업무는 다음과 같음

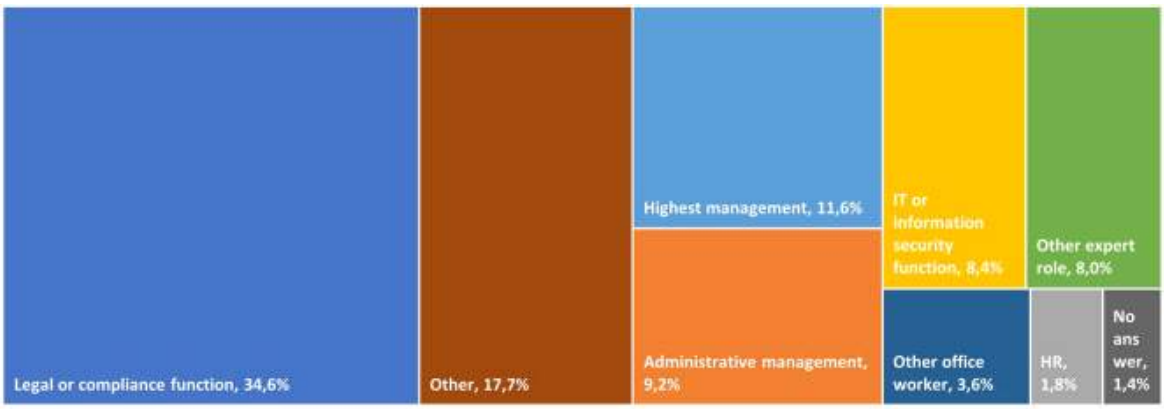
- 컨트롤러나 프로세서, 그리고 처리를 수행하는 직원에게 EU 및 회원국 개인정보보호 규정에 따른 의무에 대해 고지 및 권고
- 책임 할당, 인식 제고, 처리 작업에 관련된 직원교육 및 관련 감사 등 개인정보보호 규정과 관련한 컨트롤러 또는 프로세서의 정책 준수 현황 모니터링
- 개인정보 영향평가(Data Protection Impact Assessment, 이하 DPIA)에 관한 자문 제공 및 DPIA 이행 모니터링
- SA와의 협력 및 연락창구로써의 역할 수행

▶ **(DPO 지원)** 컨트롤러와 프로세서는 ▲DPO가 개인정보보호 관련 모든 사안에 시기적절하게 관여할 수 있도록 해야 하며 ▲DPO가 업무 수행에 있어 어떠한 지시를 받지 않도록 DPO의 독립성을 인정하고 ▲전문지식을 유지하는데 필요한 자원을 제공하는 등 DPO의 업무 수행을 지원해야 함

3. EU 역내 DPO 현황

▶ 조사에 참여한 DPO 중 70%는 조직의 내부 직원인 것으로 나타났으며, 주요 소속은 ▲법무팀·컴플라이언스팀(34.6%) ▲최고 경영진(11.6%) ▲행정관리팀(9.2%) ▲IT 및 정보보안팀(8.4%) 등 순임

표 2_ DPO 소속 부서 현황



출처: EDPB(2024)

▶ 응답자의 약 3분의 1은 DPO가 사업자단체(group of undertakings) 또는 여러 기관·단체의 단일 개인정보보호 책임자라고 답변

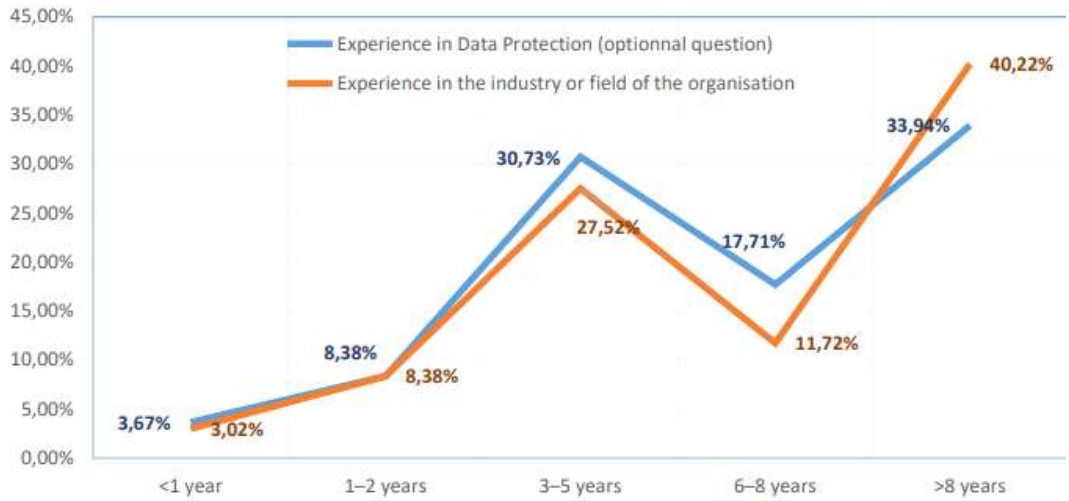
- 또한, DPO 활동을 위해 많은 경우 개인정보보호 관계 법령 및 개인정보보호 실무 지식 외에도 특정 업계 지식이 요구된다고 언급

- 실제로 대다수 DPO들은 개인정보보호 관련 역량 외에도 ▲법률(63.89%) ▲경영 프로세스(58.3%) ▲정보보안(39.3%) 등과 관련해 전문성을 갖춘 것으로 나타남

▶ 대부분의 DPO는 과거에 DPO로 근무한 경력 또는 유사 경험이 있는 것으로 확인

- DPO 경력 또는 유사 업계 경력이 3년 미만인 응답자가 13% 미만에 그친 반면, 6년 이상의 경력을 보유한 DPO는 약 50%가량으로(▲DPO 경력자 47.4% ▲관련 업계 경력자 52.25%), 신입·저연차 대비 경력직 DPO의 비율이 압도적으로 높음

표 3_ DPO 경력직 비율



출처: EDPB(2024)

4. DPO 지정 및 역할 관련 주요 이슈 및 권장 사항

▶ CEA 보고서는 동 조사를 통해 총 7가지 주요 이슈들을 식별하고 각 이슈를 개선하기 위한 권고사항들을 제시하고 있음

(1) DPO의 미지정

▶ GDPR 제37조제1항이 명시적으로 DPO 지정 의무를 부과하고 있음에도 불구하고 아직 DPO를 지정하지 않은 조직들이 존재

- 일부 공공부문에서는 해당 의무사항이 적용되지 않는다고 잘못 인식한 사례가 있었으며, 일부 응답자는 DPO 지정이 의무사항임을 인지하고 있었으나 기존 DPO 퇴사 이후 후임자를 찾지 못했다는 등의 사유로 정당성을 찾고자 한 것으로 확인

- 이에 동 보고서는 DPO 지정 의무준수에 대한 조직의 인식을 개선하기 위한 전략을 수립하고 지침 마련할 것을 권고

(2) 불충분한 DPO 자원 할당

▶ DPO의 원활한 업무 수행을 위한 예산, 시간, 인력 등의 자원이 충분하게 제공되고 있지 않은 점도 주요 이슈로 지적

- 지원 인력의 부족으로 인해 DPO가 물리적으로 처리할 수 있는 업무량에 비해 과도한 업무 수행을 요구받는 현상이 발생

- 특히 민간 부문에서는 평균적으로 91%가 DPO 업무 수행을 위한 자원이 충분하다고 응답했지만, 공공 부문의 경우 약 66%만이 자원이 충분하다고 판단

- 이러한 현상을 완화하기 위해서 조직이 DPO가 충분한 자원을 지원 받는지 평가하고 문서화하는 것이 중요

- 또한, GDPR에서 직접적으로 규정한 의무는 아니나 예산의 효과적인 관리를 위해 DPO가 자체 예산을 관리할 수 있도록 허용할 것을 권고

(3) DPO의 전문지식 및 교육 부족

▶ 조사 결과에 따르면 평균적으로 DPO가 연간 24시간의 교육을 받는 것으로 확인되었으나, 동 보고서는 각국 SA가 DPO를 대상으로 더 많은 교육과 지침을 제공할 것을 권장

- GDPR 제37조제5항이 DPO가 '전문 지식(expert knowledge)'를 갖출 것을 명시적으로 요구하고 있는 점을 강조하며, 단순 '경험(experience)'만으로는 이러한 요건을 충족할 수 없음을 지적

- 즉, 평균 90.9%의 설문 응답자가 경험 또는 전문 지식을 보유하고 있다는 사실은 응답자들이 해당 GDPR 요건을 온전히 준수하고 있음을 의미하지 않음

▶ 특히 EU 데이터 전략(European Data Strategy)의 일환으로 ▲디지털 서비스법 ▲디지털 시장법 ▲데이터 거버넌스법 ▲데이터법 ▲AI 법(안) 등 신규 법률의 추진을 고려하면 향후 DPO 교육의 중요성은 더욱 주목받을 것으로 전망

(4) 명확하지 않은 DPO 업무 할당

▶ 조사 결과에 따르면 GDPR 제39조에서 규정한 DPO의 모든 책임을 조직이 항상 DPO에게 할당하고 있지 않으며, 많은 조직이 DPO의 업무 범위에 대해 명확하게 기록한 서면 직무기술서를 보유하고 있지 않은 것으로 나타남

- 예컨대, 32.88%의 DPO는 다른 업무와 더불어 DPIA의 초안 작성 및 수행을 담당하고 있다고 응답
- 그러나 GDPR 제35조는 DPIA 수행은 DPO가 아닌 컨트롤러의 의무임을 명시하고 있기에, DPO가 DPIA 초안 작성에 상당 부분 관여할 수 있더라도 DPIA와 그 결과를 평가할 수 있는 충분한 업무적 독립성을 확보해야 함

▶ 또한, 동 보고서는 조직이 개인정보보호와 관련해 DPO와 정기적으로 협의하지 않아 조직 내 DPO의 체계적인 참여가 부족한 점을 지적

- DPO가 조직의 개인정보 처리 및 보호와 관련한 문제를 처리하거나 해결하는 데 얼마나 자주 관여 및/또는 자문을 받는가'에 대한 질문에, 응답자의 중앙값 22.54%만이 매번 자문을 받는다고 답변

▶ 이에, 컨트롤러(또는 프로세서)의 의무와 DPO의 고유 의무를 명확히 분리하고 조직 내에서 DPO의 역할의 중요성을 홍보할 것을 권고

- 아울러 컨트롤러 및 프로세서는 조직 내 DPO의 참여도를 적극적으로 검토하고 개선하기 위해 내부 지침, DPO 연간 활동 보고서, 모범 사례 등을 마련할 것을 추천

(5) 이해 상충

▶ GDPR 제38조제6항은 DPO가 고유 역할 이외의 다른 책임을 맡을 수 있도록 허용하고 있으나, DPO가 다른 직책을 겸직하고 있는 경우 이해 상충이 발생할 수 있음

- 그러나 실제로 많은 DPO가 조직의 관리 책임(예: 최고 경영진, 부서장) 역할을 겸임하고 있는 것으로 파악되었으며, 설문조사 응답자 중 절반만이 풀타임 DPO인 것으로 확인
- 최근 EU 사법재판소(CJEU)는 X-Fab 드레스덴 사례[8]를 통해 DPO의 '이해 상충(conflict of interest)'이 존재하는지를 평가하는 기준을 명확히 한 바 있으며, DPO 고유 의무의 수행을 저해할 수 있는 업무나 직무를 조직이 DPO에게 맡기지 말아야 함을 강조

8) CJEU Judgment of 9 February 2023, C-453/21, X-Fab Dresden GmbH & Co. KG, ECLI:EU:C:2023:79, para. 40-45 참고

▶ DPO가 자신의 역할에 충분한 시간을 할애할 수 있도록 ▲EDPB는 DPO에 대한 지침을 마련해야 하며 ▲각 SA는 컨트롤러와 프로세서가 DPO 역할의 이해 상충을 방지할 수 있는 적절한 안전장치를 갖추고 있는지 확인해야 함

(6) 조직 최고 경영진에 대한 DPO의 보고 미비

▶ GDPR 제38조제3항은 DPO가 조직의 최고 경영진에게 보고할 것을 요구하고 있으나, DPO는 정기적으로 보고서를 제출하지 않았으며 최고 경영진에게 접근할 수 있는 권한이 없는 것으로 나타남

- 이런 의무 준수를 강화하기 위해 SA들이 최고 경영진에 대한 DPO의 접근성 보장을 돕고, 보고 빈도와 내용에 대한 업계 표준 및 모범 사례를 담은 지침을 마련할 것을 권장

(7) DPO 역할 강화를 위한 SA 지침의 필요성

▶ 설문 응답자의 60% 이상은 DPO와 조직 내에 ▲Q&A 또는 FAQ ▲추가 가이드라인 ▲교육 자료 및 문서 등이 배포되기를 희망한다고 응답

- 다만, DPO에 대한 추가 지침을 채택하기 위해서는 이해관계자의 요구사항을 분석하고 해결하기 위한 자원확보가 필요할 것으로 보이며, 특히 소규모 SA의 경우 필요한 재정·인적 자원 확보가 필수적임

5. 결론 및 시사점

▶ 동 조사는 GDPR 준수를 위해 DPO의 역할과 인식을 강화해야 할 필요성을 제시

- 비록 개선되어야 할 사항도 있으나, DPO가 정기적인 교육을 받고 있으며 업무 수행에 필요한 기술과 지식을 갖추고 있다는 점이 확인되었다는 점은 긍정적

- SA들이 동 보고서에서 권고한 사항을 적절히 반영할 경우, DPO는 본인의 역할을 보다 효율적으로 수행하게 되어 결과적으로 많은 조직에서 겪고 있는 자원 부담을 완화할 수 있을 것으로 예상

▶ 동시에 동 보고서는 유럽 전역에 걸쳐 DPO에 대해 현행화되고 광범위한 지침이 필요하다는 점을 일관적으로 강조

- 특히 EU 데이터 전략 추진을 위해 다양한 데이터 관련 법제도가 마련된 만큼 DPO의 역할은 변화하고 있으며, 이를 통해 DPO 역할의 중요성이 더욱 강조

Reference

1. DAC Beachcroft, EDPB Coordinated Enforcement Action: Designation and Position of Data Protection Officers, 2024.2.7.
2. EDPB, 2022 Coordinated Enforcement Action: Use of cloud-based services by the public sector, 2023.1.17.
3. EDPB, 2023 Coordinated Enforcement Action: Designation and Position of Data Protection Officers, 2024.1.16.
4. EDPB, CEF 2024: Launch of coordinated enforcement on the right of access, 2024.2.28.
5. EDPB, EDPB identifies areas of improvement to promote the role and recognition of DPOs, 2024.1.17.
6. EDPB, EDPB Strategy 2021-2023, 2020.12.15.
7. Hunton Privacy Blog, CJEU Clarifies Rules on Conflict of Interest in Relation to DPO Role, 2023.2.13.
8. TLT, The European Data Protection Board's report on the role of Data Protection Officers, 2024.2.21.

〈2024년 개인정보보호 월간 동향 보고서 발간 목록〉

번호	호수	제 목
1	1월 01	EU 데이터법(Data Act) 주요 내용 분석 및 시사점
2	1월 02	EU 내 메타의 무광고 유로 서비스 모델의 개인정보 침해 이슈 분석
3	2월 01	미국 주(州) 개인정보 보호법에 대한 평가 및 분석
4	2월 02	DPO지정 및 역할에 대한 CEA 2023 조사 분석

2024

개인정보보호 월간동향분석 제2호

발 행 2024년 3월 29일

발행처 한국인터넷진흥원
개인정보본부 개인정보정책팀
전라남도 나주시 진흥길 9
Tel: 061-820-1865

1. 본 보고서는 개인정보보호위원회 「개인정보보호 동향 분석」 사업 수행 결과물입니다.
2.
3. 본 보고서의 내용은 한국인터넷진흥원의 공식 입장과는 다를 수 있습니다.