2024 Privacy Report

개인정보보호 월간동향분석

3월호

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2024 Privacy Report

개인정보보호 월간동향분석

3월호

1. 미국 백악관의 정부 데이터 및 민감 개인정보보호를 위한 행정명령 분석

2. EDPB, GDPR 주 사업장에 관한 성명 발표

KISA

미국 백악관의 민감 개인정보 보호 관련 행정명령(Executive Order 14117) 분석

[목 차]

1. 개요

2. 행정명령의 주요 내용
(1) 금지 또는 제한되는 데이터 거래에 관한 규칙제정
(2) 민감 개인정보 보호를 위한 조치
(3) 위험 평가

3. 법무부 규칙제정 사전통지의 주요 내용

4. 결론 및 시사점

1. 개요

▶ **(개요)** 바이든 대통령이 '24년 2월 28일 해외 우려국(Countries of Concern)*으로부터 미국인의 민감 개인정보를 보호하기 위한 행정명령(EO 14117)[1]을 발표

* 법무부가 발표한 '규칙제정 사전통지(Advance Notice of Proposed Rulemaking, ANPRM)'는 미국의 우려국으로 중국(홍콩, 마카오 포함), 러시아, 쿠바, 이란, 베네수엘라, 북한 6개국을 지정

- 동 행정명령은 법무부 장관에게 미국인의 민감 개인정보* 및 미국 정부 관련 데이터**가 적대국에 대량을 전송되는 것을 방지할 권한을 부여했으며, 법무부는 행정명령에 따라 '규칙제정 사전통지(ANPRM)'[2]를 3월 5일 연방관보를 통해 발행

* 개인 식별자, 지리적 위치 및 관련 센서 데이터, 생체인식 식별자, 인간 오믹스 데이터, 개인 건강정보, 개인 금융정보 또는 이들의 조합을 의미

1) Executive Order(EO) 14117 on "Preventing Access to Americans' Bulk Sensitive Data and United States Government-Related Data by Countries of Concern" (2024.2.28.)
2) National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern(2024.3.5.)

** 정보의 양에 상관없이 우려국이 미국 국가 안보를 위협하기 위해 악용할 가능성이 높다고 법무부 장관이 판단하는 민감 개인정보(군대를 포함해 연방정부의 전현직 직원이나 계약자, 고위공무원 식별에 사용될 수 있는 데이터 및 군대 등 연방정부가 통제하는 민감한 정부 사이트의 위치 정보)

▶ **(도입 배경)** 기업들이 대량으로 수집한 개인정보가 데이터 브로커*를 통해 우려국과 연계된 기업에 판매되면서 불법적 사찰, 사기, 협박 및 기타 개인정보 침해 우려가 증가하고 국가 안보와 외교 정책을 위협하고 있어 행정명령을 통한 대응 필요

* 소비자 개인정보를 수집하고 재판매할 목적으로 가공 및 분석하는 기업

- 기업들이 미국 국민의 정보를 대규모로 수집하고 데이터 브로커를 통해 합법적으로 판매 또는 재판매하는 관행이 일반화되면서 해당 데이터가 외국 정부나 정보기관, 군대가 통제하는 기업에 전달될 가능성도 증대

- 우려국이 대량의 민감 개인정보나 정부 관련 데이터를 확보할 경우, AI를 비롯한 첨단 기술을 활용해 데이터를 분석 및 조작하여 간첩 활동과 사이버작전을 벌이거나 협박과 영향력 행사 등 광범위한 악의적 활동에 참여할 수 있음

- 특히 활동가, 학자, 언론인, 반체제 인사, 정치인 등에 대한 정보를 수집함으로써 반대 의견을 억제하고 표현의 자유와 결사의 자유 및 기타 시민의 자유를 제한할 수 있음

- 현행법은 대량의 민감 개인정보에 대한 합법적 접근을 허용하고 있으며, 기존 외국인 투자위원회와 통신서비스 분야 외국인 참여 평가 위원회를 통해 사례별로 데이터 보안 위험에 대응하고 있으나 우려국이 상업적 거래를 통해 민감 개인정보에 접근함으로써 발생하는 국가 안보 위험을 포괄적으로 다루는 법률은 부재한 상황

- 이번 행정명령은 국가 안보상의 이러한 격차를 해소하기 위한 것으로, 바이든 대통령은 미국 외부에서 기인하는 국가 안보에 대한 특별한 위협을 처리하는 권한을 대통령에게 부여하는 '국제경제권한법(IEEPA)*'에 의거해 행정명령을 발행

* International Emergency Economic Powers Act: 미국의 안보, 외교, 경제에 현저한 위협이 발생할 경우 그 대상이 되는 국가와 국민의 거래 금지 등을 명할 수 있는 대통령의 권한을 규정한 법으로 1977년에 제정

2. 행정명령의 주요 내용

(1) 금지 또는 제한되는 데이터 거래에 관한 규칙제정

▶ **(금지 또는 제한되는 거래 유형)** 행정명령은 법무부 장관에게 국토안보부 장관과 협력하고 기타 관련 기관장과 협의해 다음에 해당하는 거래를 금지하거나 제한하는 규칙을 제정할 것을 요구

- 대량의 민감 개인정보 또는 미국 정부 관련 데이터를 포함하는 거래
  ※ 구체적인 사항은 동 조항에 따라 법무부 장관이 제정하는 규칙을 통해 규정

- 법무부 장관이 발행한 규칙에서 해당 거래가 대량의 민감 개인정보 또는 미국 정부 관련 데이터에 대한 우려국 또는 관련 대상자*의 접근을 허용함으로써 비상사태를 초래할 수 있다고 판단되는 거래 유형에 속하는 경우

  * Covered Person: 우려국이 소유, 통제하거나 우려국의 관할권에 있거나 지시를 받는 법인 및 법인의 직원이나 계약 관계의 외국인, 우려국의 직원 또는 계약 관계의 외국인, 우려국의 영토 관할권에 주로 거주하는 외국인. 행정명령은 또한 해당 국가의 소유나 통제를 받거나 해당 국가의 관할권에 있거나 지시를 받는 등 특정 기준을 충족하는 법인이나 개인을 대상자로 지정할 수 있는 권한을 법무부에 부여

- 법무부 장관이 발행한 규칙의 발효 시점 이후에 개시, 진행 또는 완료되는 거래

- 법무부 장관이 발행한 규칙에 의해 발급된 면허로 허가받지 않은 거래 또는 규칙에서 면제되지 않는 거래

- 법무부 장관이 발행한 규칙에서 규정된 바와 같이 금융 서비스(은행, 자본시장, 금융 보험 등) 제공에 통상적으로 수반되거나 연방 규제요건 준수에 필요한 거래가 아닌 경우

▶ **(규칙제정 시 이행사항)** 법무부 장관은 국토안보부 장관과 협력하고 기타 관련 기관장과 협의하여 행정명령 발표일로부터 180일 이내에 규칙제정안을 발표해야 하며, 규칙제정안 마련 시에는 다음의 사항을 이행 필요

- 대량의 민감 개인정보 또는 미국 정부 관련 데이터에 대한 우려국의 접근을 허용하여 국가 비상사태를 초래할 수 있는 금지된 거래 유형의 식별

- 상기 금지된 거래 유형에 속하지만, 국토안보부 장관이 CISA를 통해 수립한 보안 요구사항을 통해 대량의 민감 개인정보 및 미국 정부 관련 데이터에 대한 우려국의 접근 위험을 적절히 완화할 수 있다고 판단되는 거래 유형의 식별

- 국무부 장관과 상무부 장관의 동의를 얻어 행정명령의 목적에 따라 우려국과 관련 대상자의 등급을 식별

- 행정명령 및 세부 규칙의 영향을 받는 자들에게 규제 명확성을 제공하기 위한 체계의 확립

- 국무부 장관, 상무부 장관, 국토안보부 장관과 공동으로 금지 또는 제한된 거래에서 예외를 적용받을 수 있는 허가 제도를 마련하기 위한 절차를 수립

▶ **(규칙제정 시 고려요인)** 민감 개인정보와 정부 관련 데이터의 거래 금지나 제한을 위한 모든 규칙은 다음 사항을 고려 필요

- 대량의 민감 개인정보 또는 미국 정부 관련 데이터에 관한 거래 유형의 성격과 규모 및 기타 요소를 적절히 고려

- 해당 거래가 금지된 거래인지 또는 제한된 거래인지를 평가하는 데 사용하기 위한 기준점 및 실사(Due Diligence)* 요건을 수립

* 사업 주체가 의사 결정에 앞서 객관적인 위험 등 적합성을 평가하는 계획을 수립하고 수행할 책임

- 대량의 민감 개인정보 또는 미국 정부 관련 데이터를 미국 내에 저장하거나, 이를 처리하는 컴퓨팅 시설을 미국 내에 위치하도록 하는 광범위한 데이터 현지화 요구는 금지

- 납세자 기금으로 수행한 과학 연구 결과에 대한 공공 접근, 전자 의료정보 공유 및 상호운용성, 환자의 데이터 접근권과 관련된 미국 정부의 법적 의무를 고려

- 관련 보고서 제출 전까지는 인간 게놈 데이터* 외의 인간 '오믹스(Omic)**' 데이터 유형이 포함된 거래는 다루지 않음

* 세포에서 발견되는 유전적 지시의 전체 세트 또는 하위 세트를 구성하는 핵산 서열을 나타내는 데이터

** 인간 유전체 데이터, 후성 유전체 데이터, 단백질체 데이터, 전사체 데이터, 미생물체 데이터 또는 대사체 데이터와 같이 인간 생물학적 분자를 특성화하거나 정량화하는 인간으로부터 생성되는 데이터를 의미

- 동 조항에 따라 공포된 금지 조치는 법률이나 행정명령에 따른 규정이나 지침, 허가 제도에 의해 허용되는 범위를 제외하고 적용되며, 금지 조치를 회피 또는 위반하는 모든 거래나 기타 활동은 금지

▶ **(보안 요구사항)** 행정명령은 국토안보부 장관에게 CISA 국장을 통해 법무부 장관과 협력하고 관련 기관장과 협의해 제한된 데이터 거래로 인해 발생하는 허용할 수 없는 위험을 해결하기 위한 보안 요구사항을 마련하고 공개의견을 수렴해 발표할 것을 요구

- 보안 요구사항은 국립표준기술연구소(NIST)가 개발한 사이버보안 및 개인정보보호 프레임워크를 기반으로 하며, 국토안보부 장관은 CISA 국장을 통해 법무부 장관과 협력해 보안 요구사항에 관한 해석 지침을 발표해야 함

- 법무부 장관은 CISA 국장을 통해 국토안보부 장관과 협력하여 보안 요구사항에 관한 시행 지침을 발표해야 함

▶ **(대통령에 대한 보고)** 법무부 장관은 행정명령에 따라 발행한 규칙의 발효일로부터 1년 이내에 국무부, 재무부, 상무부, 국토안보부 장관과 협의하여 대통령에게 보고서를 제출

- 보고서는 행정명령에 기술된 국가 안보 위협을 해결하기 위해 부과된 조치의 효과 및 행정명령의 이행이 미국 산업의 국제 경쟁력에 미치는 영향을 포함한 경제적 영향에 대한 평가를 포함

※ 보고서 작성 시 법무부 장관은 행정명령이 미치는 경제적 영향에 관하여 대중의 의견을 수렴 필요

(2) 민감 개인정보 보호를 위한 조치

▶ **(네트워크 인프라 허가 검토)** 관할 네트워크 인프라를 통한 데이터 전송으로 우려국이 대량의 민감 개인정보와 미국 정부 관련 데이터에 접근할 수 있는 위험이 있기에, 미국 통신서비스 분야 외국인 참여평가 위원회*는 기존 권한과 법률에 부합하는 범위 내에서 다음과 같은 조치를 취해야 함

* The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector: 해외 소유 및 통제 통신서비스의 라이선스 기준 충족 여부에 관해 연방통신위원회(FCC)에 자문을 제공하는 기관으로 일명 '팀 텔레콤(Team Telecom)'이라고 칭함

- 우려국이 소유하거나 통제하는 기업에 의해 소유 또는 운영되거나 우려국의 관할권에서 종료되는 해저 케이블 시스템에 대한 기존 허가의 검토에 우선 착수
- 위원회 자문단과 협의하여 제3자 위험 및 우려국의 데이터 접근 평가를 포함한 허가 신청 및 기존 허가 검토에 관한 정책 지침을 발행
- 해저 케이블 시스템을 설치 또는 운영하기 위해 위원회가 검토 중인 신규 허가 신청 또는 기존 허가를 통해 우려국이 동 행정명령에 기술된 대량의 민감 개인정보에 접근함으로써 초래될 수 있는 국가 안보 및 법 집행 위험을 지속적으로 해결

▶ **(개인의 민감 건강정보 보호)** 국방부, 보건복지부, 보훈부의 장관 및 국립과학재단 이사장은 우려국이나 관련 대상자가 미국인의 민감 건강정보와 인간 게놈 데이터에 접근하는 것을 막기 위한 조치 필요

- 미국 의료시장의 기업은 의료서비스 제공업체 및 연구소와 제휴 및 계약을 통해 개인 건강정보 및 인간 게놈 데이터를 포함한 대량의 민감 개인정보에 접근 가능
- 해당 정보가 익명화, 개인화, 비식별화되어 있더라도 우려국의 대규모 데이터셋 접근 및 기술 발전으로 데이터 재식별이 가능해지면 미국인의 개인정보를 악용할 가능성이 증대
- 국방부와 보건복지부, 보훈부 장관과 국립과학재단 이사장은 법적 권한에 따라 적절한 규정, 지침, 명령 발행을 통하여 우려국이나 관련 대상자의 대량의 민감 개인정보 접근을 허용하는 보조금 지원을 금지하거나, 연방 지원 보조금 수령자에게 위협 완화를 위한 조치를 부과하여 위협에 대처 필요
- 국방부와 보건복지부, 보훈부 장관, 국립과학재단 이사장은 행정명령 발표일로부터 1년 이내에 공동으로 보고서를 대통령에게 제출해야 함

▶ **(데이터 브로커 규제)** 우려국과 관련 대상자가 데이터 브로커를 통해 대량의 민감 개인정보와 미국 정부 관련 데이터에 접근할 수 있으므로, 소비자금융보호국(CFPB) 국장은 고유권한을 행사하여 이러한 위협을 해결해야 함

- 데이터 브로커들은 미국 소비자에 관한 대량의 민감 개인정보와 정부 관련 데이터 하위집합의 수집과 집계, 평가, 배포에 관여하여 우려국의 해당 데이터 접근으로 인한 국가 비상사태에 기여할 가능성이 있음
- 따라서 CFPB는 이와 같은 위험으로부터 소비자를 보호하기 위해 연방 소비자보호법 준수를 강화하기 위한 규제를 지속적으로 추진해야 함

(3) 위험 평가

▶ **(국가 안보 위험 평가)** 행정명령에 따라 발행된 규칙의 발효일로부터 120일 이내에 법무부, 국토안보부 장관과 국가정보국장은 관련 기관장과 협의하여 대량의 민감 개인정보를 우려국으로 이전함으로써 발생하는 국가 안보 위험을 탐지, 평가, 완화하기 위한 조치를 대통령 국가안보보좌관(APNSA)에게 권고해야 함

- 행정명령에 따라 발행된 규칙의 발효일로부터 150일 이내에 대통령 국가안보 보좌관은 권고사항을 검토하고, 필요 시 법무부, 국토안보부 장관 및 관련 기관장과 권고사항의 이행에 관해 협의 필요

▶ **(인간 오믹스 데이터 관련 위험 평가)** 행정명령 발표일로부터 120일 이내에 대통령 국가안보보좌관, 국내정책위원회 국장, 과학기술정책실 국장, 팬데믹 대비 및 대응정책실 국장은 인간 게놈 데이터 이외의 오믹스 데이터와 관련된 거래 규제의 위험과 이점을 평가한 보고서를 대통령에게 제출 필요

- 보고서를 통해 해당 거래의 규제 범위를 권고해야 하며, 보고서와 권고사항 작성 시 미국 국민과 국가 안보에 대한 위험과 함께 우려국이나 관련 대상자에 대한 데이터 거래 규제에 드는 경제적, 과학적 비용도 고려 필요

3. 법무부 규칙제정 사전통지의 주요 내용

▶ 법무부는 행정명령 발표 이후 3월 5일 연방관보를 통해 '우려국에 의한 미국인의 대량의 민감 개인정보와 정부 관련 데이터에 관한 규칙제정 사전통지(ANPRM)'를 발행

▶ **(데이터 거래 금지 또는 제한 대상)** ANPRM에 따르면 법무부는 미국인과 우려국 또는 관련 대상자 간 금지 및 제한되는 데이터 거래로 다음의 범주를 고려

- (데이터 거래 금지 대상) ①데이터 중개 거래 ②대량의 인간 게놈 데이터 또는 해당 데이터에서 파생될 수 있는 생체 표본의 전송과 관련된 데이터 거래

- (데이터 거래 제한 대상) ①상품 및 서비스 제공과 관련된 공급업체 계약(클라우드 서비스 계약 포함) ②고용 계약 ③투자 계약

  ※ 제한된 데이터 거래에 적용되는 보안 요구사항은 CISA에서 마련하며, 해당 보안 요구사항은 우려국 또는 관련 대상자의 접근 위험을 완화하기 위한 것으로, 조직의 사이버보안 태세 요구사항, 물리적/논리적 접근 제어, 데이터 마스킹 및 최소화, 개인정보보호 기술 사용 등을 포함

▶ (**데이터 거래 면제 대상)** ANPRM에 따르면 법무부는 아래의 데이터 거래를 규칙 적용 대상에서 면제할 계획

- 금융 서비스나 결제처리, 규제 준수에 수반되는 경우(예: 뱅킹, 자본시장 또는 금융/보험 활동, 여타 규제기관의 관할 하의 금융 활동, 상품 및 서비스 거래를 위한 개인 금융정보나 개인식별자 관련 결제처리, 규제 준수 등)

- 통상적으로 다국적 미국 기업 내의 부수적 사업 운영(급여나 인사 등)에 수반되는 경우

- 미국 정부, 정부계약자, 직원 및 수혜자(예: 연방자금을 지원받는 보건 및 연구 활동)의 데이터 거래

- 연방법 또는 국제 협약에 의해 요구되거나 승인된 데이터 거래(예: 승객 적하목록 정보 교환, 인터폴 요청, 공중보건 감시)

▶ **("대량" 민감 개인정보의 기준점)** ANPRM에 따르면 법무부는 데이터 거래나 제한이 적용되는 대량 민감 개인정보에 대하여 위험 기반 평가를 기반으로 "대량"의 기준점을 설정할 계획으로, 위험 수준에 따라 다음과 같은 범위를 고려 중

표 1_ 민감 개인정보 거래에 대한 "대량" 기준점의 범위

위험 수준	인간 게놈 데이터	생체 식별자	정화한 지리적 위치 정보	개인 건강정보	개인 금융정보	대상 개인 식별자
낮음	100명 이상	100명 이상(생체식별자) 기기 100개 이상(위치정보)		1,000명 이상		1만 명 이상
높음	1천명 이상	1만명 이상(생체식별자) 기기 1만 개 이상(위치정보)		1백만 명 이상		1백만 명 이상

출처: 법무부 ANPRM(2024), 넥스텔리전스(주) 재구성

4. 결론 및 시사점

▶ 바이든 대통령의 이번 행정명령은 미국인의 대규모 민감 개인정보와 정부 관련 데이터가 데이터 브로커를 통해 중국이나 러시아와 같은 적대국에 판매되는 것을 방지하기 위한 목적에서 마련

- 행정명령에 따르면 이러한 거래는 특히 군대나 국가 안보 업무에 종사하는 사람들에게 개인정보 침해를 넘어 실질적인 위협을 제기하는 한편, 허용할 수 없는 국가 안보 위험을 초래 가능
- 미국 정부는 특히 적대국이 대량의 민감 정보와 정부 관련 데이터에 AI와 빅데이터 분석 등의 첨단 기술을 활용해 악의적인 활동을 전개할 가능성을 경계
- 법무부는 행정명령에 의거한 규칙제정을 통해 거래를 제한 또는 금지하는 민감한 개인정보와 정부 관련 데이터의 세부 내용을 확정할 계획으로, AI와 같은 신기술 발전에 따라 개인정보를 확보할 수 있는 데이터가 늘어나면서 규칙제정 이후에도 대상 범주가 확장될 가능성도 존재

▶ 다만 동 행정명령 자체가 기업들에게 새로운 의무를 부과하는 것이 아니라 추후 법무부가 제정하는 규칙이 신규 의무를 규정할 예정이므로, 영향을 받는 기업들은 이러한 규칙 제정 추이를 주시할 필요가 있음

- 법무부는 최종 규칙제정에 앞서 4월 말까지 두 차례에 걸쳐 공개적으로 의견을 수렴할 계획
- 법무부의 규칙이 제정되면 중국, 러시아, 이란, 북한, 쿠바, 베네수엘라와 같이 우려국으로 지정된 국가와 데이터를 거래하는 미국 기업들은 제한 또는 금지되는 거래의 유형을 파악해 대응 필요
- 특히 데이터 거래 제한 대상의 경우, CISA가 우려국의 접근 위험을 완화하기 위해 설정한 보안 요구사항을 준수해야 함

▶ 한편, 백악관은 미국이 개방된 인터넷과 국경 간 데이터 흐름을 장려한다며 이번 행정명령에 따라 대량의 민감 개인정보나 정부 관련 데이터를 미국 내에 저장하거나 처리하도록 하는 일반화된 데이터 현지화 요구사항은 부과되지 않는다고 강조

- 법무부는 금융 서비스 관련 데이터 거래와 다국적 기업의 사업 운영에 수반되는 데이터 거래, 정부기관 관련 데이터 거래 등을 규제 적용 대상에서 면제하여, 국가 안보 위험을 초래하지 않는 데이터 거래에 대한 기업의 부담을 완화할 전망

Reference

1. The White House, Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, 2024.02.28.
2. The White House, FACT SHEET: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data, 2024.02.28.
3. Department of Justice, Justice Department to Implement Groundbreaking Executive Order Addressing National Security Risks and Data Security, 2024.02.28.
4. Hogan Lovells, White House issues executive order on access to US sensitive personal data by countries of concern, 2024.03.01.
5. Data Guidance, USA: EO on preventing access to sensitive personal and government related data – breaking down the impact on transfers for businesses, 2024.03.

EDPB, GDPR 주 사업장에 관한 성명(Opinion 04/2024) 발표

[목 차]

1. 개요

2. 주 사업장의 개념 및 원스톱숍 메커니즘의 적용
(1) GDPR 제4조제16항제(호)의 문리적 해석
(2) GDPR 제4조제16항제(호)의 논리적 해석

3. EU 역내 주 사업장 식별을 위한 실질적 고려사항

4. 결론 및 시사점

1. 개요

▶ **(배경)** '24년 2월 13일, EU 개인정보보호 이사회(European Data Protection Board, 이하 EDPB)는 GDPR에 따른 컨트롤러의 주 사업장(main establishment)에 대한 개념을 확립하는 Opinion 04/2024(이하 성명서)를 발표

- 동 성명서는 컨트롤러의 주 사업장의 정의 및 원스톱숍 메커니즘[3]의 적용 기준에 대한 의견을 제시해달라는 프랑스 개인정보 감독기관(CNIL)의 요청('23.10.10.)에 따른 것임
- 특히, 주 사업장과 GDPR 전문 제36조에서 명시하고 있는 '중앙행정지점(place of central administration)'의 연관성을 명확히 한다는 점에서 의의가 있음

▶ **(주 사업장의 의의)** '주 사업장'의 지정은 컨트롤러에 대한 주된 관할권을 보유한 개인정보 감독기관이 어디인지를 결정하기에, 원스톱숍 메커니즘의 적용에 있어 중추적인 역할을 함

3) One stop shop mechanism: 처리되는 개인정보의 정보주체가 EU 내 여러 국가에 흩어져 있는 경우에 주 사업장이나 단일 사업장이 소속된 국가의 감독기관이 선임 감독기관의 역할을 수행하면서 다른 회원국의 감독기관과 수시로 협력함으로써 컨트롤러·프로세서가 하나의 감독기관만을 대상으로 대응할 수 있는 집행 체계를 지칭

- 특히 감독기관에 대한 개인정보 침해 통지 절차를 비롯해 대부분의 개인정보 처리 활동에 대해 단일 선임 감독기관(Lead Supervisory Authority, 이하 LSA)과 연락할 수 있도록 함으로써 감독기관 협력 프로세스를 간소화

표1 _ GDPR 전문 제36조

전문 제36조

컨트롤러의 EU 역내 주 사업장은 컨트롤러의 EU 내 중앙행정지점이어야 하지만, 개인정보 처리 목적 및 방식에 대한 결정을 EU 내 다른 사업장에서 내리는 경우, 그 사업장이 주 사업장으로 간주되어야 한다. 컨트롤러의 EU 내 주 사업장은 객관적인 기준에 따라 결정되어야 하며, 안정적인 방식을 통해 **처리 목적 및 방식에 대한 주요 결정을 내리는 관리 활동을 효과적이고 실제적으로 행하는 것을 의미한다**. 그 기준은 개인정보의 처리가 해당 지역에서 이루어지는지 여부에 따라 달라지지 않는다. 개인정보 처리 또는 처리 활동을 위한 기술적 수단 및 기술이 존재하고 이를 사용한다는 그 자체가 주 사업장이 되지 않으므로 이는 주 사업장을 결정하는 기준이 아니다. 프로세서의 주 사업장은 프로세서의 EU 내 중앙행정지점이거나, EU 역내에서 중앙행정처리가 이루어지지 않는 경우에는 EU 내 주요 처리 활동이 발생하는 장소가 주 사업장이다. 컨트롤러와 프로세서 모두와 관련되어 있는 경우, 선임 감독기관은 컨트롤러의 주 사업장이 있는 회원국의 감독기관이어야 하고 프로세서의 감독기관은 관련 감독기관으로 간주되어야 하며, 이 감독기관은 본 규정이 정한 협력 절차에 참여해야 한다. 어느 경우든, 프로세서의 단일 또는 복수의 사업장이 소재한 회원국 또는 복수의 회원국의 감독기관들은 결정문 초안이 컨트롤러에 한하여 관련되어 있는 경우, 관련 감독기관으로 간주되지 않는다. 사업체 집단(group of undertakings)이 처리를 수행하는 경우, 통제 사업체의 주 사업장은 사업체 집단의 주 사업장으로 간주 되어야 하며, 처리 목적과 수단을 다른 사업체가 결정하는 경우는 예외로 한다.

▶ **(CNIL 질의사항)** CNIL이 EDPB에 제기한 질의 사항은 다음과 같이 두 가지로 구성

- **(질의 1)** 컨트롤러의 EU 내 중앙행정지점이 GDPR 제4조제16항제a호에 따라 주 사업장으로 인정받기 위해, 해당 사업장이 처리의 목적과 수단에 관한 결정을 내리고 이를 실행할 수 있는 권한을 보유하고 있어야 하는가?

- **(질의 2)** 원스톱숍 메커니즘은 컨트롤러의 EU 역내 사업장 중 하나(컨트롤러의 EU 중앙행정지점)가 해당 처리 작업의 목적과 수단에 관한 결정을 내리고 그러한 결정을 이행할 권한이 있음을 입증하는 증거가 있는 경우에만 적용 가능한가?

▶ 이에 대해 EPDB는 ▲주 사업장의 법적 개념에 대한 해석을 제공하고 ▲이러한 해석을 기반으로 감독기관(Supervisory Authority, 이하 SA)이 실무에서 GDPR 제4조제16항제(a)호를 어떻게 적용해야 하는지를 명확히 하는 성명서를 공개

2. 주 사업장의 개념 및 원스톱숍 메커니즘의 적용

(1) GDPR 제4조제16항제(호)의 문리적 해석

▶ **(주 사업장의 구성 요소)** EDPB는 GDPR 제4조제16항제a호가 주 사업장의 요소 세 가지를 제시하고 있다고 분석

표2 _ GDPR 제4조제16항제(a)호

제16항 주 사업장은 다음 각 호를 의미한다. (a) **하나 이상의 EU 회원국에** 사업장을 운영하는 컨트롤러의 경우, **또 다른 사업장에서 개인정보의 처리 목적 및 처리 방식을 결정하게 할 집행권을 보유한 경우를 제외하고**, **EU 역내의 중앙행정지점을 주 사업장으로 본다**. (이하 생략)

- 동 조항이 명시한 첫 번째 조건은 컨트롤러가 **EU 회원국에 하나 이상의 사업장을 운영하고 있어야** 한다는 점
- 상기 전제조건을 충족했다는 가정 하에, 주 사업장은 ▲컨트롤러의 EU 역내 중앙행정지점이거나 ▲개인정보를 처리하는 목적과 방식에 관해 결정할 수 있는 권한과 이러한 권한을 집행할 수 있는 권한을 보유한 사업장이어야 함

▶ **(① 중앙행정지점의 정의)** GDPR이 '중앙행정지점'이라는 용어를 직접적으로 정의하고 있지 않은 관계로, EDPB는 유사한 맥락에서 주 사업장에 대해 언급하고 있는 기타 EU 법률을 참조함으로써 해당 용어가 내포하는 의미를 명확화

- **(TFEU)** EU 기능조약(Treaty on the Functioning of the European Union, TFEU) 제54조는 "회원국의 법률에 따라 설립되고 EU 내에 등록 사무소, 중앙행정지점 또는 사업장을 둔 회사 또는 기업"은 EU 국민과 동일한 방식으로 설립의 자유를 누릴 수 있음을 규정

※ TFEU 제54조의 해석과 관련하여 EU 사법재판소(CJEU)는 기업의 중앙행정지점이 해당 기업의 '실질적인 소재지'에 해당하는 것으로 간주한 사례가 있음[4)]

- **(NIS2)** 네트워크 및 정보시스템의 사이버보안 지침(NIS2 지침) 전문 제114조는 "EU에서 사이버보안 위험 관리 조치와 관련된 결정이 주로(predominantly) 이루어지는 곳"을 언급하고 있음

4) CJEU, Judgment of 27 September 1988, The Queen v H. M. Treasury and Commissioners of Inland Revenue, ex parte Daily Mail and General Trust plc., Case C-81/87, para. 21-25 참고

- **(DGA)** 데이터거버넌스법(Data Governance Act, DGA) 전문 41조는 주 사업장이 EU 역내 데이터 중개 서비스 제공자의 중앙행정지점과 일치해야 하며 "관리 활동의 효과적이고 실질적인 행사를 의미"한다고 명시

- **(DSA)** 디지털 서비스법(Digital Services Act, DSA) 전문 123조는 주 사업장에 대해 "주요 재무 기능 및 운영 통제권을 행사할 수 있는 본사 또는 등록 사무소"가 있는 장소라 언급

- 이처럼 일반적으로 기업의 중앙행정지점이 해당 기업의 가장 중요한 결정이 내려지는 곳으로 통용되는 점을 고려

▶ **(② 결정권)** 또한, EDPB는 GDPR이 개인정보 처리에 대한 결정이 컨트롤러의 EU 내 주요행정지점이 아닌 다른 EU 사업장에서 이루어지는 상황도 고려하고 있음을 주목

- GDPR은 "또 다른(another)"이라는 표현을 사용함으로써, 일반적으로 EU 역내 중앙행정지점이 ▲개인정보 처리의 목적과 수단에 관한 결정을 내리는 장소에 해당하며 ▲이러한 결정을 구현할 권한이 있다고 가정하고 있음을 분명히 함

- 즉, GDPR은 일반적으로 이러한 결정을 컨트롤러의 주요행정지점에서 내린다고 가정하고 있으나, 개인정보 처리 목적 및 방식에 대한 결정이 실제적으로 컨트롤러의 주요행정지점이 아닌 다른 EU 사업장에서 이루어지고 이행될 때에는 다른 사업장을 동 조항에 근거하여 '주 사업장'으로 간주함

▶ 따라서, 컨트롤러는 이와 같은 핵심 개인정보 처리 결정이 실제로 어디에서 시작되고 실행되는지 평가해야 힘

- 명목상 본사가 아닌 다른 EU 사업에서 이러한 결정을 내리고 이행하는 경우에는 해당 사업장이 주요행정지점을 대신하여 GDPR 상 '주 사업장'이 됨

(2) GDPR 제4조제16항제(호)의 논리적 해석

▶ EDPB는 EU 집행위원회가 본래 제안한 GDPR 초안이 "EU 내에서 개인정보 처리의 목적 조건 및 수단에 대한 결정이 이루어지지 않은 경우"에도 컨트롤러가 주 사업장을 보유할 수 있는 가능성을 명시적으로 규정하고 있던 점에 주목

- 그러나 입법 과정에서 해당 문구를 삭제한 것은, 원스톱숍 메커니즘의 혜택 대상을 EU 내에서 처리 목적과 수단에 관한 **결정을 내리고 그러한 결정을 이행할 권한을 가진** 컨트롤러로 제한하려는 의도를 암시

▶ GDPR에서 '주요행정지점'이라는 개념을 도입한 것은 개인정보 처리에 관한 주요 의사결정이 이루어지는 주 사업장을 식별하기 위한 보다 객관적이고 투명한 기준을 제공하기 위한 취지

- 다만, 이는 GDPR 제4조(16)(a)이 명시한 '주 사업장'의 범위를 확대하여 의사 결정권이 실제로 해당 사업장에 있지 않은 경우까지 고려하려는 의도는 아님
- 원스톱숍 메커니즘은 컨트롤러가 수행하는 국경 간 처리 활동에 대해 단일 감독기관(즉, LSA)과만 소통할 수 있도록 함으로써 법적 불확실성을 최소화하는 것을 목표로 함
- 이러한 맥락에서 '주 사업장'의 정의는 어느 SA가 LSA로써의 구실을 할지 결정하는 과정을 수월하게 하기 위함이라고 해석할 수 있음
- LSA는 개인정보 처리와 관련하여 실질적인 의사 결정권을 가지고 사업장에 실질적인 영향력을 행사할 수 있어야 함

▶ 따라서, 원스톱숍 메커니즘을 적용하기 위해서는 다음 사항을 증명할 수 있어야 함

- 컨트롤러의 EU 사업장 중 하나가 처리 목적과 수단에 대한 결정을 내린다는 증거 및 해당 사업장이 이러한 결정을 실행할 권한을 보유하고 있다는 증거 필요

▶ 컨트롤러의 '주요행정지점'을 식별하는 것을 시작으로, 의사결정권의 실제 위치에 따라 주 사업장의 여부 및 원스톱숍 메커니즘의 적용 여부가 결정

- 만약 이러한 의사결정권이 EU 역외에 있는 경우, 해당 결정권자는 처리에 대한 GDPR의 주 사업장에 해당하지 않음으로 원스톱숍 메커니즘이 적용 불가함

3. EU 역내 주 사업장 식별을 위한 실질적 고려사항

▶ **(입증책임)** 실질적인 개인정보 처리 관련 결정이 궁극적으로 내려지는 곳 및 EU 내에서 해당 결정을 이행할 권한이 있는 곳을 입증할 책임은 컨트롤러에게 있으며, 이러한 지정은 SA의 검토를 거쳐야 함

- 주 사업장을 지정하는 컨트롤러는 GDPR 제30조에서 명시한 처리 활동의 유효한 기록 또는 개인정보 처리방침 등 다양한 자료를 통해 다음 중 하나를 입증해야 함

① **중앙행정지점**이 처리 결정을 내리고 이를 이행할 수 있는 권한을 갖추고 있는지

② **다른 EU 사업장**이 이러한 결정을 내리고 이행할 권한을 가지고 있는지

▶ **(감독기관 검토 및 합의)** 컨트롤러는 주 사업장을 지정함에 있어 GDPR 제31조에 근거해 SA와 협력해야 하며, 관련 감독기관(Concerned Supervisory Authority, 이하 CSA)은 객관적인 기준에 따라 컨트롤러의 주 사업장 분석에 이의를 제기할 수 있음

※ CSA들은 구체적인 사례를 기반으로 적합한 세부 평가 수준에 대해 합의해야 함

- 증거를 검토하는 SA는 GDPR 제58조제1항제(a)호에 따른 권한을 사용하여 컨트롤러의 사업장에 연락하거나, 필요한 경우 GDPR 제61조에 근거한 상호 지원에 의존하여 다른 회원국 감독기관의 도움을 받아 필요한 정보를 얻을 수 있음

※ GDPR 제58조(감독기관의 권한)제1항제(a)호는 SA가 컨트롤러와 프로세서(또는 그 대리인)에 업무의 수행에 필요한 정보의 일체를 제공하도록 명령할 권한을 보유하고 있음을 명시

※ GDPR 제61조(상호 지원)은 GDPR의 시행 및 적용을 위해 SA들이 서로 관련 정보와 상호 지원을 제공하고, 상호 간의 효과적인 협력을 위한 조치를 구비할 것을 명시

- 컨트롤러가 지정한 주 사업장이 합당한지를 평가함에 있어 SA는 EU 역내에 중앙행정지점을 보유하고 있다는 사실 확인에 그치지 않고, 컨트롤러의 처리 목적 및 수단에 대한 결정이 이루어지는 곳과 이러한 결정을 이행할 수 있는 위치가 어디인지 파악해야 함

- 이와 같이 컨트롤러의 증거가 주 사업장을 입증하기에 충분한지를 검토한 후, SA는 평가 결과를 GDPR 제60조제1항에 근거하여 모든 관련 감독기관(Concerned Supervisory Authority, CSA)들과 공유해야 함

  - CSA들이 SA의 결정에 별도의 이의를 제기하지 않고 동의한 경우, 주 사업장의 지정을 통해 식별된 LSA가 주 사업장에 이러한 결정을 통지

  - CSA들이 SA의 결정에 이의를 제기한 경우에는 LSA를 식별할 수 없으므로, SA가 사업장에 이러한 사실과 원스톱숍 메커니즘을 적용할 수 없는 점을 통지해야 함

  - SA와 CSA 간에 어떠한 합의도 이루어지지 않을 경우, ▲LSA의 식별을 둘러싼 갈등(GDPR 제65조제1항제(b)호) ▲법에 관한 상이한 해석(GDPR 제64조제2항)을 근거로 EDPB에 동 사안을 회부할 수 있음

4. 결론 및 시사점

▶ 최종적으로 EDPB는 CNIL의 요청과 상기 분석에 근거하여 GDPR 제4조제16항제a호를 해석함에 있어서 다음과 같은 결론을 도출

- 컨트롤러의 EU 역내 '중앙행정지점'은 ▲개인정보 처리 목적과 수단에 대한 결정을 내리고 ▲이러한 결정을 이행할 권한이 있는 경우에만 '주 사업장'으로 간주할 수 있음

- 원스톱숍 메커니즘의 적용은 컨트롤러의 EU 역내 사업장 중 하나가 상기 두 조 건을 충족한다는 증거가 있는 경우에만 적용이 가능

▶ EDPB의 이러한 해석은 개인정보 처리에 대한 결정 및 결정 이행 권한이 EU 역외에서 이루어질 경우, 원스톱숍 메커니즘을 적용할 수 없음을 시사

- 설령 컨트롤러의 사업장이 EU 역내에 있을지라도, 해당 EU 사업장이 처리 목적 및 수단에 대한 결정을 내리지 않거나 이러한 결정을 집행할 권한을 가지고 있지 않은 경우에도 마찬가지로 원스톱숍 메커니즘을 적용할 수 없음

- 이와 같이 원스톱숍 메커니즘을 적용할 수 없는 상황에서는 각국 감독기관이 개별로 적절히 조치를 취할 수 있음을 의미

▶ 동 성명은 주 사업장을 식별할 의무가 있는 기업들에게 법적 확실성을 제공한다는 점에서 의의가 있으며, 감독기관의 관할권과 기업이 EU 전반에 걸쳐 개인정보를 처리하는 방식에 영향을 미칠 것으로 전망

- 기업들은 EDPB가 제시한 기준에 따라 기업의 중앙행정지점 및 본사를 정확히 파악하고, 이로써 개인정보 처리와 관련해 협력해야 할 LSA가 어디인지 인지하고 있는 것이 중요

- 또한 해당 시설이 '주 사업장'이라는 주장을 추후 뒷받침하기 위해서는 기업의 개인정보 처리 활동에 관한 결정이 어디에서 이루어지고 있는지와, 그러한 결정을 실행할 권한이 어디에 있는지를 입증하는 증거를 확보해두어야 함

- 이와 같이 조치하지 않을 경우, 기업들은 개인정보 침해에 대응하고, 최대 27개국의 감독기관들과 개별로 소통해야 한다는 번거로움에 직면할 가능성이 있음

▶ 동 성명은 EU에 지사를 두고 있지만 주요 의사 결정이 EU 역외 국가에서 집중적으로 이루어지는 글로벌·영국 기업들에 중요한 지침으로 작용할 것

- 증거 기반 의사 결정과 이행 능력의 중요성을 강조하며, 컨트롤러에게 원스톱숍 메커니즘의 적용을 입증할 책임을 부여하는 EDPB의 해석은 EU에서 사업을 운영하는 해외 조직에 상당한 영향을 미칠 것이며, GDPR 준수를 위한 조직의 역할과 책임에 대한 세심한 평가의 필요성을 강조함

Reference

1. EDPB, EDPB clarifies notion of main establishment and calls on EU legislators to make sure CSAM Reuglation respects rights to privacy and data protection, 2024.2.14.
2. EDPB, Opinion 04/2024 on the notion of main establishment of a controller in the Union under Article 4(16)(a) GDPR, 2024.2.13.
3. JDSUPRA, EDPB adopts opinion on the notion of main establishment during 90th plenary, 2024.2.22.
4. Mayson Hayes & Curran, European Data Protection Board Clarifies the One Stop Shop Test, 2024.2.28.

〈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
5	3월 01	미국 백악관의 정부 데이터 및 민감 개인정보보호를 위한 행정명령 분석
3	3월 02	EDPB, GDPR 주 사업장에 관한 성명 발표

2024
개인정보보호
월간동향분석 제3호

발 행 2024년 3월 29일

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