한국 기업에 대한 GDPR의 적용

2019년 5월 21일

고려대학교 법학전문대학원
정명현

GDPR의 영토적 적용범위

- GDPR 제3조: 영토적 범위

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. 3. …	1. 본 규칙은, 처리가 EU 역내외에서 발생하는지 여부에 관계없이, EU 내의 컨트롤러 또는 프로세서의 사업장의 활동 맥락에서 개인정보의 처리에 적용된다. 2. 본 규칙은, 처리 활동이 다음에 관련된 경우, EU 내에 설립되지 않은 컨트롤러 또는 프로세서에 의한 EU 내의 정보주체의 개인정보의 처리에 적용된다: (a) 정보주체의 지불이 요구되는지 여부와 관계없이, EU 내의 이러한 정보주체에게 상품이나 서비스의 제공; 또는 (b) 그들의 행동이 EU 내에서 발생하는 한 그들 행동의 감시. 3. …

GDPR의 역내적용

- 대상: EU 내 컨트롤러 또는 프로세서의 '사업장의 활동 맥락에서' 수행되는 개인정보 처리 (사업장 기준)
- 개인정보의 처리가 EU 역내·외에서 발생하는지 여부에 관계없이 EU 내 사업장에 적용
  - EU 내의 컨트롤러나 프로세서의 사업장의 활동 맥락에서 EU 내에서 개인정보가 처리되면 당연히 적용됨.
  - EU 내의 컨트롤러나 프로세서의 사업장의 활동 맥락에서 EU 역외에서 개인정보가 처리되어도 적용됨.
    - 사업장은 '안정적 방식을 통한 활동의 효과적이고 현실적인 수행'을 의미: 지점, 지사, 합작회사등
    - 지점이나 지사와 같은 법적 형식은 사업장인지 여부의 결정에 중요하지 않음.

GDPR의 역내적용

- 한국에 본사를 둔 자동차 제조업체가 마케팅 홍보 등 EU 내 활동 관리를 위해 벨기에 브뤼셀에 지사를 두는 경우
  - 브뤼셀 지사는 자동차 제조업체가 수행하는 경제적 활동의 성격을 고려하여 실제적이고 효과적인 활동을 수행하는 안정적 방식이라고 볼 수 있고, 따라서 이 브뤼셀 지사는 GDPR 제3조에 따른 EU 내 사업장으로 볼 수 있음
- 한국 기업이 운영하는 전자상거래 웹사이트가, 개인정보는 한국에서 처리하면서 EU시장을 타겟으로 마케팅 활동을 위하여 벨기에 브뤼셀에 사무소를 설립한 경우
  - EU시장을 타겟으로 하는 마케팅 활동이 전자상거래 웹사이트의 서비스를 제공하기 위한 것이라면, 브뤼셀 사무소의 활동은 한국의 전자상거래 웹사이트가 수행하는 개인정보 처리와 불가분의 관계라고 볼 수 있음.
  - 따라서 한국 기업의 개인정보 처리는 EU 내 사업장으로서 브뤼셀 사무소의 활동 맥락에서 수행되는 것으로 볼 수 있음. GDPR이 적용됨.

GDPR의 역내적용

- 프랑스 기업이 개발한 한국의 소비자를 대상으로 하는 차량 공유 앱 서비스가 한국에서 이용 가능하지만, 모든 개인정보의 처리는 프랑스의 컨트롤러에 의하여 수행되는 경우
  - 개인정보의 수집은 EU 역외에서 수행되지만 동 개인정보의 추후 처리는 EU 내 컨트롤러의 사업장의 활동 맥락에서 수행됨. 이 경우 EU에 소재하지 않는 정보주체의 개인정보에 관련되지만, 프랑스 기업이 수행한 개인정보 처리에 GDPR이 적용됨
- 스웨덴 스톡홀름에 본사를 둔 제약회사가 임상시험 데이터에 관한 모든 개인정보 처리 활동을 한국에 소재한 지점에서 수행하는 경우
  - 스톡홀름 본사가 독립된 법적 실체가 아닌 한국 지점이 수행하는 개인정보 처리의 목적과 수단을 결정한다면, 개인정보 처리는 한국에서 수행되지만 동 처리는 스톡홀름에 소재한 제약회사, 즉 EU에 설립된 컨트롤러의 활동 맥락에서 수행되므로, 동 처리에 GDPR이 적용됨

GDPR의 역외적용

- 대상: 'EU 내 소재하는 정보주체'의 개인정보 (표적기준)
- GDPR은 EU 내에 설립되지 않은 컨트롤러나 프로세서에 의한 EU 내 정보주체의 개인정보 처리에도 적용될 수 있음
  - EU 내 정보주체에게 상품이나 서비스를 제공하는 경우 (정보주체의 지불여부 불문)
  - EU 내 정보주체에 대해 EU 내에서 발생하는 행동을 감시하는 경우
- 정보주체의 법적 지위에 따라 제한되지 않음
  - '국적 또는 거주지와 관계없이'(상설 14항)
  - '국적이나 영주권, 또는 기타 유형의 법적 지위에 의해 제한되지 않음'(가이드라인)
- 정보주체의 EU 내 소재 요건은 관련행위의 발생시점 기준
  - 개인정보 처리활동의 기간에는 관계가 없음.

GDPR의 역외적용

- EU 내 정보주체에 대한 상품 또는 서비스의 제공
- 컨트롤러나 프로세서가 EU 회원국 내의 정보주체를 '겨냥하여'(directed) 상품 또는 서비스 제공을 의도하고 있음이 분명하게 확인되어야 함.
    - EU에서 컨트롤러, 프로세서 또는 중개자 웹사이트, 이메일 주소 또는 다른 연락처의 단순한 접속 가능성이나 컨트롤러가 설립된 제3국에서 일반적으로 이용되는 언어의 사용은 이러한 의도를 확인하기에 충분하지 않을 것임.
    - 하나 이상의 EU 회원국에서 일반적으로 이용되는 언어나 통화로 재화나 서비스를 주문할 가능성이 있거나, EU 내의 소비자나 이용자를 언급하는 경우에는, 해당 컨트롤러가, EU 내 정보주체에게 상품이나 서비스 제공을 예상하는 것으로 볼 수 있음.
    - 개인정보 개념에 온라인 식별자가 명시적으로 포함됨으로써, EU 역외에서 EU 내 정보주체에게 온라인 판매, 게임프로그램 등을 제공하는 온라인 서비스 제공자나 온라인 분석 서비스 제공자에 대한 GDPR 적용이 명확해짐
        - 이 경우 EU 역외 프로세서, 예컨대 한국의 외주 개인정보 처리 기업도 해당함
        - 이 경우 EU 역외에 거주하는 EU시민의 개인정보 처리는 해당하지 않음

GDPR의 역외적용

- 상품 또는 서비스의 제공이 EU 내 사람을 '겨냥한'(directed) 것인지 판단 시 고려 요소

- 제공되는 상품 또는 서비스와 관련하여 EU 또는 최소한 하나의 회원국을 명시적으로 지정
- EU 내에서 소비자들이 사이트에 쉽게 접속할 수 있도록, 컨트롤러 또는 프로세서가 인터넷 레퍼런스서비스 검색엔진 운영자에게 비용 지불; 또는 컨트롤러나 프로세서가 EU 국가를 대상으로 마케팅 및 광고 캠페인 개시
- 해당 활동의 국제적 성격, 예컨대 관광서비스 제공
- EU 회원국으로부터 연락 받을 수 있는 전용 주소 또는 전화번호의 언급
- 컨트롤러 또는 프로세서가 설립된 제3국의 도메인이 아닌 '.de'와 같은 최상위 도메인네임 사용 또는 '.eu'와 같은 중립적인 최상위 도메인네임 사용
- EU 회원국으로부터 서비스가 제공되는 곳으로의 여행에 대한 설명
- 여러 EU 회원국들에 거주하는 소비자들로 구성된 국제적 고객에 대한 언급, 특히 그러한 고객들이 작성한 게시글 등 근거 제시
- 상품 및 서비스 제공자의 국가에서 일반적으로 사용되는 언어나 통화 이외의 언어 또는 통화 사용, 특히 하나 이상의 EU 회원국의 언어 또는 통화 사용
- 컨트롤러가 EU 회원국에 상품 배달서비스 제공

GDPR의 역외적용

- EU 내에서 발생하는 정보주체의 행동의 감시에 관련되는 경우
  - 개인정보 처리 활동이 정보주체의 행동을 감시한다고 판단하기 위하여 해당 자연인이 인터넷상에서 추적되는지가 확인되어야 함.
    - 특히 정보주체에 관한 결정을 내리기 위하여 또는 그의 개인적 선호, 행태 및 태도를 분석하거나 예측하기 위하여 정보주체를 프로파일링하는 개인정보 처리 기법 등의 잠재적인 추후 이용이 포함됨.
    - 개인정보 처리를 포함하는 다른 유형의 네트워크나 기술을 통한 추적, 예컨대 웨어러블이나 기타 스마트 디바이스를 통한 경우도 고려
    - 모든 온라인 개인정보 수집이나 분석이 자동적으로 감시가 되는 것은 아니며, 개인정보의 처리 목적과 개인정보를 포함하는 추후 행동 분석 또는 프로파일링 기술에 대한 고려 필요
    - 행태 관련 광고, 마케팅 목적의 지리적 기반 활동, 쿠키 또는 지문을 이용한 온라인 추적, 맞춤형 온라인 건강분석 서비스, 개인 프로파일에 기초한 설문조사 등 감시활동 포함

GDPR의 역외적용

- 한국에 설립된 스타트업 기업이 EU 내 사업장을 두지 않고 유럽과 미주 지역을 방문하는 관광객들을 위해 해당 관광지의 시내 지도 어플리케이션을 제공하는 경우
  - 동 어플리케이션은 이를 사용하는 고객들이 방문하는 도시에서 일단 어플리케이션을 사용하기 시작하면, 관광명소, 음식점, 호텔 등에 대한 표적 광고를 제공하기 위해 사용자의 위치에 대한 개인정보를 처리하고, 관광객들이 뉴욕, 샌프란시스코, 토론토, 런던, 파리, 로마를 방문하는 동안 사용이 가능하도록 구성되어 있음.
  - 또한 이 스타트업 기업은 시내지도 어플리케이션을 통하여 EU 내의 개인(특히 런던, 파리, 로마)에게 서비스를 제공함.
  - 이러한 서비스의 제공과 관련하여 EU에 소재하는 정보주체의 개인정보를 처리하는 것은 제3조 제2항에 따라 GDPR의 적용 범위에 해당됨.

GDPR의 역외적용

- 한국 시민이 휴가기간 중에 유럽을 여행하면서, 유럽에 있는 동안 한국 회사가 제공하는 새로운 어플리케이션을 다운로드하여 이용하는 경우
  - 이 어플리케이션이 한국 시장을 겨냥한 것이라면, 한국 회사가 이 프로그램을 통해 한국 여행자의 개인정보를 수집하더라도 GDPR의 적용 대상이 아님
- 한국의 은행이 한국 내에 거주하는 독일 시민에게 서비스를 제공하는 경우
  - 해당 은행이 국내에서만 활동하고 EU 시장을 표적으로 하지 않는다면, 한국의 은행이 독일 시민의 개인정보를 처리하더라도 GDPR의 적용 대상이 아님
- 캐나다 이민국이 비자 심사 목적으로 캐나다에 입국하는 EU 시민의 개인정보를 처리하는 경우
  - 이러한 처리에는 GDPR이 적용되지 않음.

EU역외 기업의 EU 내 대리인의 지정

- GDPR 제27조: EU 내에 설립되지 않은 컨트롤러 또는 프로세서의 대리인

1. 제3조 제2항이 적용되는 경우, 컨트롤러 또는 프로세서는 EU 내 대리인을 서면으로 지정하여야 한다.
2. 이 의무는 다음에 적용되지 않는다:
(a) 간헐적이고, 대규모로 제9조 제1항에 언급된 특수한 범주의 개인정보의 처리 또는 제10조에 언급된 범죄경력 및 범죄행위에 관련된 개인정보의 처리를 포함하지 않으며, 처리의 성격, 문맥, 범위와 목적을 고려하여 자연인의 권리와 자유에 대한 위험을 초래할 것 같지 않은 처리; 또는
(b) 공공당국 또는 기관.
3. 대리인은 정보주체가 소재하고, 상품 또는 서비스의 그에게 제공과 관련하여 개인정보가 처리되거나 그의 행동이 감시되는 회원국들 중 하나에 설립되어야 한다.
4. 대리인은, 컨트롤러 또는 프로세서와 함께 또는 이에 대신하여, 본 규칙의 준수를 보장하기 위한 목적으로 처리와 관련한 모든 쟁점에 대하여 특히 감독당국과 정보주체를 상대하도록, 컨트롤러 또는 프로세서에 의하여 권한이 부여되어야 한다.
5. 컨트롤러 또는 프로세서의 대리인 지정은 컨트롤러 또는 프로세서 자신에 대하여 개시될 수 있는 법적 조치에 영향을 미치지 않는다.

EU역외 기업의 EU 내 대리인의 지정

- GDPR의 역외 적용을 받는 컨트롤러 또는 프로세서는 EU 내에 대리인을 지정하여야 함.
  - 대리인(representative)은 컨트롤러 또는 프로세서에 의하여 서면으로 지정됨.
  - GDPR에 의무에 관하여 컨트롤러 또는 프로세서를 대리하는 EU에 설립된 자연인 또는 법인을 의미함.
- 대리인 지정의무의 면제 : 개인정보 처리의 성격, 맥락, 범위 및 목적을 고려하여, 그 처리가
  - (i) 간헐적이고, (ii) 대규모로 특별한 범주의 개인정보 (민감정보)의 처리를 포함하지 않거나 대규모로 범죄 경력에 관련된 개인정보의 처리를 포함하지 않으며, (iii) 자연인의 권리와 자유에 위험을 초래할 우려가 없는 경우
  - 공공당국 또는 공공기관이 개인정보를 처리하는 경우
- 대리인은 정보주체가 소재하고, 정보주체에게 상품이나 서비스의 제공 또는 정보주체의 행동에 대한 감시와 관련하여, 해당 개인정보가 처리되는 회원국 중 하나에 설립되어야 함.
  - 회원국 감독당국은 대리인을 지정하지 않은 컨트롤러나 프로세서에게 최대 1천만 유로 또는 사업자의 경우 이 금액과 전년도 세계매출액의 2% 중에서 더 큰 금액의 과징금을 부과할 수 있음.

EU역외 기업의 EU 내 대리인의 지정

- 대리인의 의무와 책임
- 대리하는 컨트롤러 또는 프로세서와 정보주체 사이의 연락 원활
- 처리 활동의 기록 유지
- GDPR의 준수를 보장하기 위한 목적으로 취해진 조치에 관하여 소관 감독당국과 협력
  - 컨트롤러(프로세서)는 처리와 관련한 모든 쟁점에 대하여 대리인이 감독당국과 정보주체를 상대하도록 권한을 부여해야 함.
- 감독당국의 직무 수행에서 그의 요청에 따라 감독당국과 협력해야 함.
  - 컨트롤러 또는 프로세서의 대리인이 회원국 감독당국의 요청에 협력하지 않은 경우 감독당국은 컨트롤러나 프로세서에게 최대 1천만 유로 또는 사업자의 경우 이 금액과 전년도 세계매출액의 2% 중에서 더 큰 금액의 과징금을 부과할 수 있음.
- 대리인의 지정은 컨트롤러 또는 프로세서에 대하여 제기될 수 있는 법적 조치 (소송)에 영향을 주지 않음

EU역외 기업의 EU 내 대리인의 지정

- 한국에 소재하고 관리되는 웹사이트가 영어, 프랑스어, 네덜란드어 및 독일어로 이용 가능하고 유로나 파운드로 결제되며, 맞춤형 가족사진 앨범의 편집, 출력 및 배송 서비스를 제공하는 경우
  - 동 웹사이트가 해당 앨범을 우편으로 영국, 프랑스, 벨기에, 네덜란드, 룩셈부르크 및 독일에서만 배달되는 것으로 나타내면, 동 웹사이트는 GDPR 제3조 제2(a)항에 따라 GDPR의 적용을 받게 됨.
  - 이 경우 해당 컨트롤러는 EU에 대리인을 지정하여야 하는데, 대리인은 영국, 프랑스, 벨기에, 네덜란드, 룩셈부르크, 또는 독일 중 한 회원국에 설립되어야 함.

EU역외 기업의 EU 내 대리인의 지정

- EU에 사업 실재나 사업장을 두지 않았으나 GDPR 제3조 제2항에 따라 GDPR의 역외 적용을 받는 한국의 제약회사의 경우
  - 동 회사가 벨기에, 네덜란드 및 룩셈부르크의 병원들이 수행하는 임상시험을 지원하고
  - 임상시험에 참여하는 환자들 다수는 벨기에에 소재한다면
  - 컨트롤러인 한국의 제약회사는 동 임상시험에 참여하는 환자들인 정보주체가 소재하는 이들 세 회원국들 중의 하나에 설립되는 대리인을 지정해야 함.
  - 환자들 대부분이 벨기에에 거주하기 때문에 동 대리인은 벨기에에 설립되겠지만, 벨기에에 설립된 대리인은 네덜란드와 룩셈부르크의 정보주체들과 감독당국들에게도 용이하게 접근 가능하도록 해야 함.

GDPR에 대한 대응

- GDPR이 적용되는지 여부를 확인하고
  - EU 내 사업장의 활동 맥락에서 한국에서 개인정보가 처리되는지, 또는
  - EU에 설립되지 않더라도 EU에 서비스나 상품을 제공하는지, 또는
  - EU에 설립되지 않더라도 EU 내의 개인의 행동을 감시하는지 여부
- GDPR의 내용을 올바르게 이해하여야 하며
  - 기업 내 모든 임직원이 GDPR의 기본원칙을 이해하고 준수해야 할 책임을 인식해야 함.
    - GDPR의 적용대상인 개인정보의 개념을 이해하여야 함.
    - GDPR이 규정한 개인정보보호원칙과 정보주체의 권리를 이해하여야 함.
    - GDPR이 규정한 컨트롤러와 프로세서, 즉 개인정보를 처리하는 기업의 의무를 이해하여야 함.
    - GDPR에서 허용된 개별 회원국의 관련 법의 내용도 이해하여야 함.
- GDPR을 성실하게 준수하여야 함
  - EU역외 기업도 필요한 경우 대리인을 지정하고, 또한 개인정보 처리 활동을 기록하는 등 GDPR의 요구사항을 실행하여야 함.
  - GDPR의 규정 위반으로 과징금이 부과되면, 개인정보 유출 등으로 사회적 평판이 낮아질 수 있음.

감사합니다

chungmh@korea.ac.kr