연구논문

EU 개인정보보호법의 영토적 적용 범위에 관한 고찰

박 노 형*
정 명 현**

EU의 개인정보보호법으로서 2018년 5월 25일부터 적용되고 있는 일반개인정보보호규칙(GDPR)은 국제법상 영토주권의 원칙에 따라 EU 내 컨트롤러와 프로세서에게 적용되는 것이 원칙이지만, EU 내 정보주체의 개인정보보호를 위하여 EU 역외 컨트롤러나 프로세서에게도 광범위하게 적용된다. 개인정보의 처리에 관하여 EU에 영향을 주는 경우에, 온라인 서비스 제공자 등 EU 역외에서 개인정보의 처리를 수반하는 사업자는 GDPR을 준수해야 한다. GDPR의 영토적 적용 범위는, 그 전신인 1995년 EC지침과 달리, EU 역외에 설립되어 EU 역내의 처리수단을 이용하지 않는 컨트롤러나 프로세서가 EU 내 정보주체에게 상품이나 서비스를 제공하거나 EU 내에서 발생하는 정보주체의 행동을 감시하는 경우의 개인정보 처리로 확대된다. 이러한 적용범위를 명확히 하기 위하여 2018년 11월 16일 유럽개인정보보호이사회(EDPB)는 'GDPR의 영토적 범위에 관한 가이드라인 3/2018'을 채택하였다.

GDPR의 영토적 적용 범위의 확대는 세계적인 데이터 이동의 맥락에서 EU 정보주체 권리의 종합적인 보호를 보장하고 개인정보보호 요건의 준수에 있어서 EU시장에서 활동하는 기업들에게 공평성을 확립하기 위한 것이다. GDPR의 역외 적용은 EU의 새로운 개인정보보호 프레임워크의 가장 혁신적인 내용이면서, 실제로 가장 어려운 쟁점이 되고 있다. GDPR의 역외 적용을 포함하여, 영토적 적용 범위에 관한 EDPB의 가이드라인은 영토적 적용 범위에 관한 해석에서 중요한 지침이 된다. GDPR의 영토적 적용 범위의 해석과 적용은 특히 한국 등 EU 역외에 설립된 기업 등에게 실무적으로 어려운 문제가 되고 있다. 한국 기업이 EU에 소재하는 정보주체에게 상품이나 서비스를 제공하는 경우 등에서 정보주체의 개인정보를 처리하는 활동에 관하여 GDPR의 적용을 받는지 확인하고, GDPR의 적용을 받아야 하는 경우 GDPR의 관련 규정을 위반하여 제재 등의 불이익을 받지 않아야 할 것이다. 이 점에서 GDPR의 관련 규정의 본문은 물론 상설과 특히 영토적 적용 범위에 관한 EDPB의 가이드라인에 대한 올바른 이해가 요구된다.

주제어: EU 개인정보보호법, GDPR, 영토적 적용범위, 역외적용, 대리인

* 고려대학교 법학전문대학원 교수(wtopark@korea.ac.kr, 주저자)
** 고려대학교 법학전문대학원 강사(chungmh@korea.ac.kr, 교신저자)

목 차

I. 서론

2018년 5월 25일 적용되기 시작한 EU의 개인정보보호법인 '일반개인정보보호규칙'(General Data Protection Regulation, 이하 'GDPR'이라 함)[1]은 국제법상 영토 주권의 원칙에 따라 EU 내의 컨트롤러와 프로세서에게 적용되는 것이 원칙이

1) GDPR의 원명은 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC'이다.

지만, EU 내 정보주체의 개인정보보호를 위하여 EU 역외의 컨트롤러나 프로세서에게도 광범위하게 적용된다.[2] 개인정보의 처리에 관하여 EU에 영향을 주는 경우에 EU 역외에서 개인정보의 처리를 수반하는 사업자, 특히 인터넷 기반 사업자는 GDPR을 준수해야 한다. GDPR의 영토적 적용 범위는, 그 전신인 1995년 지침 95/46/EC (이하 'EC지침'이라 함)과 달리, EU 역외에 설립되어 EU 역내 '처리 수단의 이용'(use of equipment)을 하지 않는 컨트롤러나 프로세서가 EU 내 정보주체에게 상품 또는 서비스를 제공하거나, EU 내에서 발생하는 정보주체의 행동을 감시하는 경우의 개인정보 처리로 확대된다. 2018년 11월 16일 유럽개인정보보호이사회(European Data Protection Board: EDPB)는 'GDPR의 영토적 범위에 관한 가이드라인 3/2018'(이하 '가이드라인'이라 함) 초안을 채택하고,[3] 2019년 1월 19일까지 대중의 의견수렴기간을 가졌다. GDPR의 영토적 적용 범위의 확대는 세계적인 데이터 이동의 맥락에서 EU 정보주체 권리를 종합적으로 보호하고, 개인정보보호 요건의 준수에 있어서 EU시장에서 활동하는 기업들에게 공평성을 확립하기 위한 것이다.[4] 또한, GDPR의 적용을 받는 EU 역외 컨트롤러나 프로세서는 EU 내에 그 대리인(representative)을 지정하여야 한다.[5]

GDPR의 영토적 적용 범위는 크게 사업장(establishment)과 표적화(targeting)의 두 가지 기준에 따르는데,[6] 이들 두 기준의 어느 하나에 해당하면, 해당 컨트롤러

2) EU의 개인정보보호에 관한 법의 적용에서 중요한 개념 중의 하나는 개인정보를 처리하는 컨트롤러(controller)와 프로세서(processor)이다. GDPR 제4조 제7호와 제8호에서 각각 컨트롤러는 '단독으로 또는 타인과 공동으로 개인정보 처리의 목적과 수단을 결정하는 자연인이나 법인, 공공당국, 에이전시 또는 다른 기관'이라고 정의되고, 프로세서는 '컨트롤러를 대신하여 개인정보를 처리하는 자연인이나 법인, 공공당국, 에이전시 또는 다른 기관'이라고 정의된다. 컨트롤러는 한국의 개인정보보호법의 개인정보처리자에 상응하는 것으로 이해되기도 하는데, 개인정보보호법이 개인정보 처리의 양태에 중심을 둔다면, GDPR은 개인정보 처리의 결정에 중심을 두고 있다. 이 점에서 이들 두 개념은 엄밀하게는 동일하다고 볼 수 없다. 컨트롤러는 프로세서, 즉 타인에게 개인정보 처리를 위탁하는 점에서 개인정보보호법의 위탁자와 유사하다고 볼 수 있지만, 개인정보보호법의 위탁자는 개인정보를 직접 수집하여 수탁자에게 그 처리를 위탁하는데, GDPR의 컨트롤러는 개인정보 처리의 목적과 수단을 결정하면 되고 개인정보를 직접 수집할 필요가 없는 점에서 차이가 있다. 이 점에서 컨트롤러가 개인정보보호법의 개인정보 처리 위탁자보다 넓은 개념이라고 볼 수 있다. 컨트롤러와 위탁자의 개념에 차이가 있으므로, 프로세서와 수탁자의 개념에도 차이가 있다고 볼 것이다. 박노형 외 8인, EU 개인정보보호법 -GDPR을 중심으로-, 박영사, 2017, 34-39쪽 참조. 컨트롤러와 프로세서의 개념에 관하여 Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP169 (2010년 2월 16일 채택) 참조.

3) European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation* (2018년 11월 16일 채택).

4) 가이드라인 3쪽. 한국의 개인정보보호 관련법은 영토적 적용 범위에 관한 명시적 규정을 두지 않는다.

5) GDPR 제27조.

6) 각각 GDPR 제3조 제1항과 제2항 참조.

나 프로세서의 개인정보 처리에 GDPR이 적용된다. 이러한 명백한 기준에도 불구하고, GDPR의 영토적 적용 범위의 해석과 적용은 특히 한국 등 EU 역외에 설립된 기업 등에게 실무적으로 어려운 문제가 되고 있다. 개인정보 처리 활동에서 수용할 수 없는 윤리적 문제가 있는 경우 EU 영토가 '데이터 피난처'(data haven)로 이용될 수 없고, EU에 설립된 프로세서는 컨트롤러의 소재지에 관계 없이 EU의 개인정보 보호에 관한 법은 물론 공공질서에 관하여 EU와 회원국의 법도 준수해야 한다.[7] 물론 이 경우 GDPR 제3조 제2항에 따라서도 GDPR의 영토적 적용 범위에 해당하지 않는 EU 역외에 설립된 컨트롤러에게는 추가적 의무가 부과되지 않는다. 아래에서 EDPB의 가이드라인을 중심으로 GDPR 제3조의 영토적 적용 범위를 분석한다.

II. GDPR의 EU 역내 컨트롤러와 프로세서에 대한 적용

GDPR은 개인정보의 처리가 EU 역내·외에서 발생하는지 여부에 관계없이, EU 내 컨트롤러 또는 프로세서 사업장의 활동 맥락에 따른 개인정보의 처리에 적용된다.[8] 따라서, GDPR은 개인정보의 처리가 EU 역내에서 발생하는 경우는 물론, EU 내 컨트롤러나 프로세서의 사업장의 활동 상황에 따라 EU 역외에서 발생하는 개인정보 처리에도 적용된다.

1. EU 역내 사업장

GDPR은 개인정보의 처리가 EU 역내·외에서 발생하는지 여부에 관계없이, EU 내 컨트롤러 또는 프로세서 사업장의 활동 맥락에 따른 개인정보의 처리에 적용된다. GDPR은 둘 이상의 회원국에 사업장을 가진 컨트롤러 또는 프로세서에 대한 감독당국을 결정하기 위하여 그의 '주된 사업장'(main establishment)의 정의를 규정하지만, 사업장 자체에 대한 정의를 규정하고 있지는 않다.[9] 다만, 사업장은 '안정적 방식을 통한 활동의 효과적이고 현실적인 수행'(effective and real exercise of activity through stable arrangements)을 암시한다고 한다.[10] 예컨대, 지점,

7) 가이드라인 12쪽.
8) GDPR 제3조 제1항.
9) 주된 사업장의 정의는 GDPR 제4조 제16호, 총괄 감독당국의 권능은 GDPR 제56조 참조.
10) GDPR 상설 제22항.

지사나 합작회사는 사업장이 될 수 있지만, 이동 중인 판매원은 사업장으로 보기 어렵다.[11] 그러나, 이러한 지점이나 자회사 등의 법적 형식은 사업장의 결정 요소가 되지 못한다.[12]

EU사법법원은 사업장의 개념을 '안정적 방식을 통하여 행사되는, 최소의 경우라도, 실제적이고 효과적 활동'(any real and effective activity – even a minimal one– exercised through stable arrangements)으로 확대한다.[13] EU 역외에 소재한 실체가 EU회원국에 사업장을 가지고 있는지 판단하기 위해서는, '경제적 활동의 특정 성격과 해당 서비스의 제공'(the specific nature of the economic activities and the provision of services concerned)에 관하여, 해당 사업체가 설립되지 않은 회원국에서의 '그러한 방식의 안정성과 활동의 효과적 수행'(the degree of stability of the arrangements and the effective exercise of activities)이 고려된다.[14] 이러한 점은 특히 전적으로 인터넷을 통하여 서비스를 제공하는 사업체의 경우에 중요하다.[15] 그럼에도, 컨트롤러의 활동 중심이 온라인으로 서비스를 제공하는 경우 안정적 방식의 문턱은 상당히 낮을 것이라고 한다.[16] 예컨대, EU 역외 실체의 대리인 한 명이 충분히 안정적으로 활동한다면 이 경우에도 안정적 방식으로 인정될 수 있다.[17]

또한, 개인정보 처리에 책임이 있는 EU 역외 실체가 EU회원국에 지점이나 자회사를 두고 있지 않은 경우에도 사업장의 존재가 인정될 수 있다. 그러나, 사업체의 웹사이트가 EU에서 접근 가능하다는 이유만으로 EU 역외 실체가 EU 내에 사업장을 가지고 있다고 결론을 내릴 수는 없다.[18] 즉, 사업장의 개념은 광범위하지만 나름의 제한이 있는 것이다. 예컨대, 한국에 본사를 둔 자동차 제조업체가 마케팅과 홍보 등 EU 내 활동을 관장하기 위하여 벨기에 브뤼셀에 지사를 두는 경우, 동 브뤼셀 지사는 자동차 제조업체가 수행하는 경제적 활동의 성격을 고려하여 실제적이고 효

11) White & Case, *Unlocking the EU General Data Protection Regulation*, 2017, p. 15.

12) GDPR 상설 제22항.

13) *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság* (C- 230/14, 2015년 10월 1일 결정), para. 31 (이하 '*Weltimmo v. NAIH*'이라 함). 동 사건은 헝가리 감독당국이 EC지침을 전환한 국내법에 따라 Weltimmo에게 부과한 과징금에 관한 헝가리 국내재판에서 EC지침의 관련 규정의 해석에 관한 예비적 결정이다.

14) *Weltimmo v. NAIH*, para. 29.

15) *Weltimmo v. NAIH*, para. 29.

16) 가이드라인 5쪽.

17) *Weltimmo v. NAIH*, para. 30.

18) *Verein für Konsumenteninformation v. Amazon EU Sarl*, (C- 191/15, 2016년 7월 28일 결정), para. 76. 동 사건은 룩셈부르크에 설립된 소비자정보협회(VKI)와 Amazon 사이의 소송에서 오스트리아 최고법원이 EU기능조약(TFEU) 제267조에 따라 제기한 예비적 결정의 요청에 따른 것이다.

과적인 활동을 수행하는 안정적 방식이라고 볼 수 있다. 따라서, 동 브뤼셀 지사는 GDPR 제3조에 따른 EU 내 사업장으로 고려할 수 있다.[19]

컨트롤러 또는 프로세서가 EU 내에 설립된 것이라면, GDPR 제3조 제1항의 적용 여부를 결정하기 위하여 개인정보 처리가 이 사업장의 활동 맥락에서 수행되는지 결정하여야 한다. EU 역외에 설립된 컨트롤러 또는 프로세서가 EU회원국 영토에서 안정적 방식을 통하여 최소이더라도 실제적이고 효과적 활동을 수행한다면, 컨트롤러나 프로세서는 동 방식의 법적 형식이 지사나 자회사인지에 관계없이 이 회원국에 사업장을 가진 것으로 고려될 수 있다.[20] 따라서, 아래와 같이, 사업장의 '활동 맥락에서' 개인정보가 처리되는지 검토하는 것이 중요하다.

2. 사업장의 '활동 맥락에서' 수행되는 개인정보 처리

GDPR 제3조 제1항에 따라 컨트롤러 또는 프로세서가 GDPR의 적용을 받기 위해서는 관련 EU의 사업장 자체가 해당 개인정보를 처리할 필요는 없고, 해당 처리가 컨트롤러나 프로세서의 해당 사업장의 '활동 맥락에서'(in the context of the activities) 수행되면 된다. 이와 관련하여 EDPB는 EU에 소재한 실체가 GDPR 제3조 제1항의 목적으로 컨트롤러 또는 프로세서의 사업장으로 고려되는지의 결정은 개별 사례에서 구체적으로 분석되어야 한다고 권고한다.[21] 즉, GDPR 제3조 제1항의 '컨트롤러 또는 프로세서의 사업장의 활동 맥락에서 처리'의 의미는 관련 판례에 따라 이해될 수 있다. 그러나, 정보주체의 효과적이고 완전한 보호를 보장하기 위하여 '사업장의 활동 맥락에서'의 의미는 제한적으로 해석될 수 없다.[22] 또한, EU 역외 실체의 '개인정보 처리 활동과 가깝지도 않은 연결을 가진 [EU 내] 모든 사업장'(any and all establishments with the remotest links to the data processing activities)의 존재에 의하여 EU법 즉, GDPR이 적용된다고 너무 넓게 해석되어서도 안 된다.[23] 즉, EU 회원국 내에서 EU 역외 실체의 상업적 활동이 개인정보 처리

19) 가이드라인 5쪽.

20) *Weltimmo v. NAIH*, para. 29.

21) 가이드라인 6쪽.

22) *Weltimmo v, NAIH*, para. 25 및 *Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (C-131/12, 2014년 5월 13일 결정), para. 53 (이하 '*Google Spain*'이라 함). *Google Spain*사건은 스페인 감독당국의 소위 잊힐 권리의 집행에 대한 *Google Spain* 등의 불복으로 야기된 스페인 법원이 제기한 예비적 결정의 요청에 따른 사건이다.

23) Article 29 Data Protection Working Party, *Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain*, WP179 update (2015년 12월 16일 채택, 이하 'WP

와 너무 동떨어진(so far remove) 경우에는, 해당 상업적 활동의 존재가 GDPR 범위 내에서의 개인정보 처리가 되기에 충분하지 않을 수 있다.[24]

EU회원국 내 현지 사업장의 활동과 EU 역외에 설립된 컨트롤러 또는 프로세서의 개인정보 처리 활동은 '불가분의 관계여서'(inextricably linked) 현지 사업장이 실제로는 해당 개인정보 처리에서 아무런 역할을 하지 않는 경우에도 EU법이 적용될 수 있다.[25] 사안별 분석에서 EU 내 사업장의 활동과 EU 역외 컨트롤러나 프로세서의 개인정보 처리 사이에 불가분의 관계가 드러나면, EU 내 사업장이 동 개인정보 처리에서의 역할에 관계없이 EU 역외 실체의 개인정보 처리에 EU법이 적용된다.[26]

EU 내 현지 사업장의 수익 활동이 EU 역외에서의 개인정보 처리와 EU 내 개인과 불가분의 관계로서 고려될 수 있는 경우, 이 수익 활동은 EU 사업장의 활동 맥락에서 수행되고 있는 EU 역외 컨트롤러 또는 프로세서의 개인정보 처리를 나타낼 수 있어서, EU법이 적용되기에 충분하다.[27] 따라서, EU에 판매사무소 등의 실재를 가지고 있는 EU 역외 사업자의 경우, 동 사무소가 실제로 개인정보 처리에 아무런 역할을 하지 않더라도, 개인정보 처리가 EU에서의 판매 활동의 맥락에서 수행되고 동 사업장의 활동이 사업장이 소재한 EU회원국의 거주자들을 대상으로 하는 경우, GDPR이 적용되는 것이다.[28]

EDPB는 EU 역외 기관들의 경우 첫째, 개인정보가 처리되고 있는지 결정하고, 둘째, 개인정보가 처리되는 활동과 EU 내 해당 기관의 실재의 활동 사이의 잠재적 관련을 확인하여 동 처리 활동을 평가하도록 권고한다.[29] 예컨대, 개인정보 처리 활동은 한국에서만 수행하면서 EU시장을 목표로 마케팅 활동을 위하여 벨기에 브뤼셀에 사무소를 설립한 한국 소재 기업이 전자상거래 웹사이트를 운영하는 경우, EU시장을 목표로 하는 마케팅 활동이 전자상거래 웹사이트가 제공하는 서비스를 제공하기 위한 것이라면, 브뤼셀 사무소의 활동은 한국의 전자상거래 웹사이트가 수행하는 개인정보 처리와 불가분의 관계라고 볼 수 있다. 이 때 한국 기업의 개인정보 처리는 EU 내 사업장으로서 브뤼셀 사무소의 활동 맥락에서 수행되는 것으로 고려할 수 있

179 update'라 함), p.5.
24) WP179 update, p. 5, foot note 13.
25) *Google Spain*, para. 56 참조.
26) WP179 update, p. 4.
27) *Id.*, pp. 4-5.
28) *Id.,* p. 5, foot note 12.
29) 가이드라인 7쪽.

어서, GDPR 제3조 제1항에 따라 GDPR이 적용된다.[30] 한편, 한국 소재 호텔이 웹사이트를 통하여 영어, 독일어, 프랑스어 및 스페인어로 패키지 서비스를 제공하는 경우, 동 호텔이 EU 내에 사무소 등 어떤 안정적 방식도 가지지 않으면, 한국의 호텔, 즉 컨트롤러에 연결된 실체는 EU 내 사업장으로 볼 수 없고, 이러한 개인정보 처리는 GDPR 제3조 제1항에 따른 GDPR의 적용을 받지 않는다.[31]

3. 개인정보의 EU 역내·외에서의 처리에 관계없이 EU 내 사업장에 대한 GDPR의 적용

GDPR 제3조 제1항은 GDPR이 개인정보의 '처리가 EU 역내·외에서 발생하는지 여부에 관계없이'(regardless of whether the processing takes place in the Union or not) EU 내 사업장의 활동 맥락에서의 동 처리에 적용된다고 규정한다. EU 내 컨트롤러나 프로세서의 사업장을 통한 실재, 그리고 개인정보의 처리가 동 사업장의 활동 맥락에서 발생한다는 사실에 의하여 개인정보 처리에 대한 GDPR의 적용이 가능하게 된다. 따라서 EU 사업장의 활동 맥락에서 수행된 개인정보 처리가 GDPR의 적용 범위에 해당하는지의 판단에서 개인정보 처리의 장소는 관련이 없다.[32]

예컨대, 프랑스 기업이 한국의 소비자를 대상으로 하는 차량 공유 앱 서비스를 개발하였고 이 서비스를 한국에서 이용할 수 있지만, 모든 개인정보의 처리는 프랑스의 컨트롤러에 의하여 수행되는 경우, 개인정보의 수집은 EU 역외에서 수행되지만 이 개인정보의 추후 처리는 EU 내 컨트롤러의 사업장의 활동 맥락에서 수행된다. 따라서 개인정보 처리는 EU에 소재하지 않는 정보주체의 개인정보에 관련되지만, GDPR은 프랑스 기업이 수행한 개인정보 처리에 적용된다.[33] 한편, 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

30) 가이드라인 7쪽.

31) 가이드라인 7쪽. 이 경우 한국 호텔이 아래에서 검토되는 GDPR 제3조 제2항에 따라 GDPR의 역외 적용을 받는지 별도로 검토되어야 한다.

32) 가이드라인 8쪽. GDPR의 영토적 적용 범위의 결정에서 지리적 장소는 다음의 사업장 소재에 관하여 중요하게 된다: 컨트롤러 또는 프로세서가 EU 역내 또는 역외에 설립되는지; 및 EU 역외 컨트롤러 또는 프로세서의 사업상 실재로서 EU에 사업장을 가지는지. 그러나, 개인정보의 처리가 수행되고 있는 장소나 해당 정보주체의 소재에 관하여는 지리적 장소는 중요하지 않다. 가이드라인 9쪽.

33) 가이드라인 8쪽.

한국에서 수행되지만 동 처리는 스톡홀름에 소재한 제약회사, 즉 EU에 설립된 컨트롤러의 활동 맥락에서 수행되므로, 이러한 개인정보 처리에는 GDPR이 적용된다.[34]

GDPR은 EU 내 개인의 개인정보 처리에 국한하여 적용되는 것은 아니다. 이와 관련하여 EDPB는 EU 내 컨트롤러나 프로세서의 사업장의 활동 맥락에서 개인정보 처리는, 해당 개인정보의 정보주체의 국적이나 소재에 관계없이, GPPR의 적용 범위 내에 해당한다고 간주한다.[35] 즉, GDPR이 제공하는 보호는 국적이나 거소지에 관계없이 그의 개인정보 처리에 관련하여 자연인에게 적용된다.[36]

4. 컨트롤러와 프로세서에 대한 사업장 기준의 적용

다른 기관(고객 기업)을 위하여 또는 다른 기관의 지시에 따라 개인정보를 처리하는 기관은 고객 기업, 즉 컨트롤러에 대한 프로세서가 된다. 컨트롤러와 프로세서 사이의 관계의 확립 요건은 컨트롤러나 프로세서가 설립된 지리적 장소에 따라 달라지지는 않지만, EDPB는 GDPR에 따른 컨트롤러와 프로세서의 다른 의무를 확인하기 위하여 각 실체의 처리가 개별적으로 고려되어야 한다는 입장이다.[37] 이와 관련하여 EDPB는 EU 내 프로세서는 그 자체의 지위를 이유로 컨트롤러의 사업장으로서 고려되어서는 안된다고 판단한다.[38]

GDPR의 적용을 받는 컨트롤러가, EU 역외 소재의 GDPR의 적용을 받지 않는 프로세서를 이용하는 경우, 컨트롤러는 계약 등으로 프로세서가 GDPR에 따라 개인정보를 처리하도록 보장할 필요가 있다.[39] 따라서 컨트롤러는 GDPR의 적용을 받는 프로세서에게 부과되는 의무를, 계약을 통하여 이러한 프로세서에게 부과할 수 있다. GDPR의 적용을 받지 않는 프로세서는 이러한 계약을 통하여 GDPR의 적용을 받는 컨트롤러에 의하여 부과되는 일정한 의무를 간접적으로 따르게 된다.

예컨대, 러시아에 거주하는 소주 민족인 사미인(Sami people)을 연구하는 핀란

34) 가이드라인 8쪽.
35) 가이드라인 9쪽.
36) GDPR 상설 제14항.
37) 가이드라인 제9쪽. 즉, EU에 설립된 프로세서는 GDPR이 프로세서에 부과한 의무를 준수해야 하고, 프로세서에게 지시하는 EU에 설립된 컨트롤러는 GDPR이 컨트롤러에게 부과한 의무를 준수해야 한다. 컨트롤러에 대한 프로세서의 지위에 관하여 GDPR 제28조 참조.
38) 가이드라인 9쪽.
39) GDPR 제28조 제3항은 프로세서의 개인정보 처리는 계약 또는 다른 법적 행위에 규율된다고 규정한다.

드의 연구소가 이 연구를 위하여 한국에 소재한 프로세서를 이용하는 경우, GDPR은 공식적으로 한국의 프로세서에게 직접 적용되지 않지만, 핀란드의 연구소, 즉 컨트롤러는 개인정보의 처리에서 GDPR의 요건을 충족하는 방식으로 적절한 조치를 취하도록 충분히 보장하고 정보주체의 권리 보호를 보장하는 프로세서만을 이용할 의무를 가진다. 따라서 핀란드 컨트롤러가 한국의 프로세서와 체결하는 개인정보 처리 약정에서 이러한 프로세서의 의무가 규정될 것이다.[40]

컨트롤러의 사업장과 달리 프로세서의 EU 내 사업장의 활동 맥락에서 수행되는 개인정보 처리의 효과는 덜 분명하다. 이 점에서 EDPB는 컨트롤러와 프로세서의 사업장은 분리해서 고려하는 것이 중요하다고 강조한다.[41] 우선, 컨트롤러가 EU 내 자신의 사업장 맥락에서 개인정보를 처리하는 것으로 고려되지 않는 경우, 동 컨트롤러는 GDPR 제3조 제1항에 따라 GDPR이 컨트롤러에게 부과하는 의무의 적용을 받지 않는다.[42] 이 경우 프로세서의 EU 내 사업장은 동 컨트롤러에 관하여 사업장으로 고려되지 않는다.[43] 또한, 프로세서가 EU 내 사업장의 맥락에서 개인정보를 처리하는 경우, 동 프로세서는 GDPR이 프로세서에게 부과하는 의무의 적용을 받는다. 그러나, 이 경우 EU 역외 컨트롤러에게는 GDPR이 컨트롤러에게 부과하는 의무가 적용되지 않는다. 즉, EU 내 프로세서를 이용한다는 이유로 동 EU 역외 컨트롤러가 GDPR의 적용을 받는 것은 아니다.[44]

GDPR의 적용을 받지 않는 컨트롤러가 EU 내 프로세서에게 지시하더라도 EU 내 프로세서의 활동 맥락에서 개인정보 처리를 수행하는 것은 아니다. 동 처리는 컨트롤러 자신의 활동 맥락에서 수행되고, 프로세서는 단지 처리 서비스를 제공하는 것이며, 동 처리 서비스는 컨트롤러의 활동과 불가분의 관계를 가지는 것은 아니다.[45] EU 역외에 설립되어 GDPR 제3조 제2항에 따른 GDPR의 역외 적용을 받지 않는 컨트롤러를 대신하여 EU 내 프로세서가 개인정보를 처리하는 경우, 동 컨트롤러의 처리 활동은, 단지 EU에 설립된 프로세서가 자신을 대신하여 처리한다는 이유로, GDPR의 영토적 적용 범위 내에 해당하는 것으로 간주되지 않는다.[46] 그러나 이렇게 컨트롤러가 EU 내에 설립되지 않고 GDPR 제3조 제2항에 따른 GDPR의 역외

40) 가이드라인 10쪽.
41) 가이드라인 10쪽.
42) 물론 동 컨트롤러는 GDPR 제3조 제2항에 따라 GDPR의 역외 적용의 대상이 될 수 있다.
43) 가이드라인 10쪽.
44) 가이드라인 10쪽.
45) 가이드라인 10쪽.
46) 가이드라인 11쪽.

적용을 받지 않더라도, EU 내에 설립된 프로세서는 GDPR 제3조 제1항에 따라 GDPR의 적용을 받는다.[47] 이 경우 동 프로세서는 EU 또는 해당 회원국의 법에 따른 다른 의무도 준수하여야 한다. 특히 프로세서는 컨트롤러의 지시가 GDPR이나 다른 EU 또는 회원국의 개인정보보호 규정을 위반한다는 의견이면 컨트롤러에게 고지하여야 한다.[48]

예컨대, 한국의 소매회사는 한국 시장을 상대로 활동을 하는 중에, 스페인에 설립된 프로세서와 계약을 체결하여 자신의 고객 개인정보를 처리하게 할 수 있는데, 이 처리가 EU 역외에 소재한 정보주체에 관한 것이고, 동 한국 소매회사가 자신의 상품이나 서비스 제공을 통하여 EU 영토 내의 개인을 표적으로 하지 하지 않고 그러한 개인의 행태를 감시하지도 않는 경우, EU 역외 설립 컨트롤러의 개인정보 처리는 GDPR 제3조 제2항에 따라서도 GDPR의 적용을 받지 않는다. 그러나, 동 개인정보 처리는 스페인에서 수행되기 때문에 이 프로세서는 자신의 활동 맥락에서 수행된 개인정보 처리에 관하여 GDPR의 적용을 받는다.[49]

EU 역외에 설립되어 GDPR 제3조 제2항에 따라서도 GDPR의 영토적 적용 범위 내에 들지 않는 컨트롤러를 위하여 개인정보 처리를 수행하는 프로세서는, 프로세서에 적용되는 GDPR의 다음 규정의 적용을 받는다: 프로세서의 주된 의무에 관한 제28조 제2항 내지 제6항, 프로세서의 권한에 따른 처리에 관한 제29조, 처리 보안에 관한 제32조 제4항, 처리 활동 기록에 관한 제30조 제2항, 감독당국과의 협력에 관한 제31조, 처리 보안에 관한 제32조, 감독당국에게 침해 신고에 관한 제33조, 개인정보보호책임자에 관한 제37조, 개인정보보호책임자의 지위에 관한 제38조, 개인정보의 역외 이전에 관한 제V장.

III. GDPR의 EU 역외 컨트롤러와 프로세서에 대한 적용

EU 내에 사업장이 없더라도 제3국에 설립된 컨트롤러나 프로세서가 GDPR의 적용 범위에서 제외되는 것은 아니다. 제3조 제2항은 “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 관

47) 가이드라인 11쪽.
48) GDPR 제28조 제3(h)항 참조.
49) 가이드라인 11쪽.

계없이, EU 내의 이러한 정보주체에게 상품이나 서비스의 제공; 또는 (b) 그들의 행동이 EU 내에서 발생하는 한 그들 행동의 감시."라고 하여 GDPR의 역외적용을 규정한다. 따라서, 그 처리 활동에 따라 EU에 설립되지 않은 컨트롤러나 프로세서에게도 GDPR이 적용된다.[50]

EDPB는 가이드라인에서 GDPR의 영토적 범위를 명확히 하면서 컨트롤러와 프로세서가 EU 또는 회원국들의 분야별 법제와 국내법 등 다른 적용 가능한 문서들을 함께 고려할 필요가 있다고 강조한다.[51] 실제로 GDPR의 여러 조항들은 회원국들이 추가적인 조건을 도입하고, 특정 분야나 처리 상황과 관련하여 국내적 차원에서 특정 개인정보보호 프레임워크를 정의할 수 있도록 허용하고 있다. 따라서 컨트롤러와 프로세서는 개별 회원국이 도입한 상이한 추가적인 조건과 프레임워크를 인식하고 이에 합치하도록 하여야 한다.[52]

EU 내에 소재하는 정보주체에 대한 '표적 기준'(targeting criterion)의 적용은, EU 내에 설립되지 않은 컨트롤러 또는 프로세서에 의해 수행되는 상품 또는 서비스의 제공, 또는 EU 내 정보주체에 대한 행동 감시에 관련된 처리 활동에 의해 개시될 수 있으며, 이 표적 기준은 '처리 활동'이 '관련되어 있는' 것이 무엇인지에 집중한다.[53] 동 기준의 적용 조건을 판단함에 있어 EDPB는, 첫째, 처리가 EU 내에 소재하는 정보주체의 개인정보에 관련된 것인지, 둘째, 처리가 EU 내 정보주체에게 상품 또는 서비스의 제공 또는 EU 내 정보주체의 행동의 감시에 관련된 것인지를 판단하기 위하여 이중의 접근방식을 권고한다.[54]

---

50) GDPR 제3조 제2항. EDPB는 EU 내 사업장이 없는 경우에, 컨트롤러나 프로세서는 제56조에 규정된 원스톱샵(one-stop shop) 메커니즘의 혜택을 받을 수 없다는 점을 재확인하고 있다. 가이드라인 12쪽. 원스톱샵 메커니즘은, EU 내에 하나 이상의 사업장을 두고 있는 컨트롤러 또는 프로세서가 국경간 개인정보를 처리하는 경우, 컨트롤러 또는 프로세서의 주된 사업장의 감독당국이 GDPR 제60조에 규정된 협력절차에 따라 총괄 감독당국이 되고, GDPR 위반이나 민원이 제기되는 경우 총괄 또는 지정된 감독당국에서 그 절차를 단일하게 진행할 수 있도록 마련된 제도이다. GDPR 제56조 참조. 이와 같이 GDPR의 협력 및 일관성 메커니즘은 EU 내에 사업장을 두고 있는 컨트롤러와 프로세서에게만 적용되는 것이며, EU 내에 사업장이 없이 회원국 내에 대리인을 두고 있는 것만으로는 원스톱샵 시스템이 적용되지 않는다. Article 29 Data Protection Working Party, *Guidelines for identifying a controller or processor's lead supervisory authority,* WP 244 rev.01 (2016년 12월 13일 채택, 2017년 4월 5일 개정), pp.9-10.

51) 가이드라인 12쪽.

52) 이와 같이 회원국법에 따라 추가적인 조건을 규정할 수 있도록 허용한 GDPR의 규정에는, 아동이 정보사회서비스에 의한 자신의 개인정보 처리에 관하여 유효한 동의를 할 수 있는 연령을 13세부터 16세 사이로 정할 수 있도록 한 제8조, 특수한 범주의 개인정보 처리에 관한 제9조 등이 있다.

53) 가이드라인 12쪽.

54) 가이드라인 12쪽.

1. EU 역내 정보주체

GDPR의 역외적용 규정은 그 적용 대상으로서 'EU 내 소재하는 정보주체의 개인정보'를 규정한다. 따라서 정보주체에 대한 표적 기준의 적용은 개인정보가 처리되는 정보주체의 국적이나 영주권, 또는 기타 유형의 법적 지위에 의해 제한되지 않는다.[55] GDPR 상설은 "이 규칙에 의해 부여된 보호는, 국적 또는 거주지(place of residence)와 관계없이 개인정보의 처리와 관련된 자연인에게 적용된다."고 하여 이러한 해석을 뒷받침하고 있다.[56] GDPR의 적용 대상이 EU 시민에만 국한되지 않는다는 이러한 규정과 해석은 개인정보의 보호에 관한 권리를 모두에게 광범위하게 인정하는 EU 기본권헌장(Charter of Fundamental Right of the European Union)을 반영한 것이다.[57] 또한 정보주체가 EU 내에 소재하여야 한다는 요건은, 이 기준을 발동시키는 관련 행위가 발생하는 시점을 기준으로 평가되어야 한다. 예컨대, 상품 또는 서비스의 제공 시점, 또는 정보주체의 행동이 감시되는 시점 등이다. 상품 또는 서비스의 제공 기간이나 행동의 감시가 이루어진 기간에는 관련이 없다.[58]

예컨대, 한국에 설립된 스타트업 기업이 EU 내 사업장을 두지 않고 유럽과 미주 지역을 방문하는 관광객들을 위해 해당 관광지의 시내 지도 앱을 제공하는 경우에, 이 앱은 이를 사용하는 고객들이 방문하는 도시에서 일단 앱을 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 있다. 또한 이 스타트업 기업은 시내지도 앱을 통하여 EU 내의 개인(특히 런던, 파리, 로마)에게 서비스를 제공한다. 따라서 이러한 서비스의 제공과 관련하여 EU에 소재하는 정보주체의 개인정보를 처리하는 것은 제3조 제2항에 따라 GDPR의 적용 범위에 속하게 된다.[59]

또한 EU 내 개인의 개인정보를 처리한다는 사실만으로는 EU 역외 컨트롤러나 프로세서의 처리 활동에 GDPR을 적용하기에 충분하지 않다. EU 내 정보주체에게 상품 또는 서비스를 제공하거나, 그들의 행동에 대한 감시를 통해, EU 내 개인에 대한 표적의 요소가 추가로 요구된다. 따라서, 제3국에서 이루어지는 EU 시민 또는 거주

55) 가이드라인 13쪽.
56) GDPR 상설 제14항.
57) EU 기본권헌장 제8조는 개인정보의 보호에 관한 권리는 제한되지 않고 '모두'(everyone)를 위한 것이라고 규정하고 있다.
58) 가이드라인 13쪽.
59) 가이드라인 13쪽.

자의 개인정보 처리는, 그러한 처리가 EU 내 개인에 대한 특정한 서비스 제공이나 EU 내 개인에 대한 감시와 관련되지 않는 한, GDPR이 적용되지 않는다.[60] 예컨대, 한국 시민이 휴가기간 중에 유럽을 여행하는 동안, 한국 회사가 제공하는 새로운 앱을 다운로드하여 이용하는 경우, 이 앱이 한국 시장을 겨냥한 것이라면, 한국 회사가 이 프로그램을 통해 한국 여행자의 개인정보를 수집하더라도 GDPR의 적용 대상이 아니다.[61] 한편, 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 아니다. 캐나다 이민국이 비자 심사 목적으로 캐나다에 입국하는 EU 시민의 개인정보를 처리하는 경우에도 그러한 처리에는 GDPR이 적용되지 않는다.[62]

2. EU 역내 정보주체에 대한 상품 또는 서비스 제공

GDPR의 역외적용을 발동하는 첫 번째 활동은 '상품 또는 서비스의 제공'이다. 서비스의 제공은 정보사회서비스의 제공을 포함하는데, 정보사회서비스는 '전자적 수단으로 서비스 수령자의 개별적 요청에 따라, 원격지에서 보통 대가를 조건으로 제공되는 서비스'라고 정의된다.[63] 상품 또는 서비스의 제공에 관한 표적 기준은, 정보주체의 지불이 요구되는지에 관계없이 적용된다. 따라서 EU 내에 설립되지 않은 컨트롤러나 프로세서의 활동이 상품 또는 서비스의 제공으로 간주되는지는, 상품 또는 서비스의 제공을 대가로 정보주체의 지불이 있었는지 여부에 의존하지 않는다. EU사법법원은 네덜란드 정부가 해외에서 전송된 프로그램에 광고 및 자막을 금지하는 규제에 대하여 네덜란드 광고협회가 제소한 사건에서, 케이블 회사의 서비스 제공이 있었는지를 판단함에 있어, 방송국이 자사 프로그램을 방영하는 케이블회사에게 비용을 지불하였는지 여부는 관계가 없다고 판단하였다.[64]

60) 가이드라인 14쪽.
61) 가이드라인 14쪽.
62) 가이드라인 14쪽.
63) Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services Article 1(b), "any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."
64) *Bond van Adverteerders and Others vs. The Netherlands State,* CJEU, C-352/85, 26 April 1988, par. 16.

표적 기준의 첫 번째 활동이 충족될 수 있는지 여부를 판단하는 다른 핵심 요소는, 상품 또는 서비스의 제공이 EU 내 사람을 '목표한'(directed) 것인지 여부이다. 달리 말하면, 컨트롤러 또는 프로세서의 행위가 EU 내 소재하는 정보주체에게 상품 또는 서비스를 제공하려는 의도를 증명하는지 여부이다.[65] 컨트롤러 또는 프로세서가 EU 내에 소재하는 정보주체에게 상품 또는 서비스를 제공하고 있는지를 판단하기 위해서는, 컨트롤러나 프로세서가 EU 내 하나 이상의 회원국 내의 정보주체에게 서비스를 제공할 것을 예견하였음이 명백한지가 확인되어야 한다.[66] 단지 EU 내에서 컨트롤러나 프로세서 또는 중개업자의 웹사이트, 이메일주소 또는 기타 연락처 세부사항에 접속할 수 있다거나, 또는 컨트롤러가 설립된 제3국에서 일반적으로 사용되는 언어를 사용한다는 사실만으로는, 그러한 의도를 확인하는 데 충분하지 않다. 반면에 하나 이상의 EU 회원국에서 일반적으로 사용되는 언어 또는 통화(currency)를 사용하고 해당 언어로 상품과 서비스를 주문할 수 있는지, 또는 EU 내 소비자 또는 이용자에 대한 언급이 있는지 등의 요소를 통하여, 컨트롤러가 EU 내 정보주체에게 상품 또는 서비스를 제공할 것을 예견하였는지를 명확하게 할 수 있을 것이다.[67] 이와 관련하여 '규칙 44/2001'[68], 특히 제15조1(c)항에 근거한 다음의 EU사법법원 판결이 유용할 것이다. *Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller*[69] 사건에서 EU사법법원은 EU규칙 44/2001(Brussels I) 제15조1(c)항의 의미 내에서 '활동을 목표하는'(to direct activity)의 의미에 관하여, 거래업자가 동 규칙 제15조 제1항의 의미 내에서 자신의 활동이 소비자의 주소가 있는 회원국을 '목표하고'(directing) 있는 것으로 간주될 수 있는지를 판단하기 위해서 거래업자가 그러한 소비자와 상업적 관계를 수립할 의도를 명백히 했어야 한다고 판시하였다. 동 맥락에서 EU사법법원은 거래업자가 회원국 내 주소를 둔 소비자들과 비즈니스를 할 것을 예견하고 있었다는 것을 입증할 수 있는 증거를 고려하였다.[70]

---

65) 가이드라인 15쪽.

66) GDPR 상설 제23항.

67) GDPR 상설 제23항.

68) 관할권 및 민사와 상사 문제에서 판결의 승인과 집행에 관한 규칙 44/2001.

69) *Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller,* Judgment of the Court (Grand Chamber) of 7 December 2010 (references for a preliminary ruling from the Oberster Gerichtshof (Austria)) — Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09) (Joined cases C-585/08 and C-144/09).

70) *Id.*, para.2.

'활동의 목표'(directing an activity) 개념은 '상품 또는 서비스의 제공'과 구별되지만, *EDPB*는 *Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller*[71] 사건의 판시가 상품이나 서비스가 EU 내 정보주체에게 제공되었는지 여부를 고려할 때 도움이 될 수 있다고 보았다. 따라서 각각의 사례에서 특히 다음의 요소들이 고려될 수 있고, 이는 서로 결합하여 고려할 수 있다.[72]

- 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 비용을 지불하거나, 컨트롤러 또는 프로세서가 EU 국가를 대상으로 마케팅 및 광고 캠페인 개시
- 해당 활동의 국제적 성격, 예컨대 관광서비스 제공
- EU 회원국으로부터 연락받을 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 또는 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

또한 GDPR의 역외적용이 개시되는 활동과 '관련된'(related) 처리 활동도 GDPR의 영토적 범위에 포함된다. 이때 처리활동과 상품 또는 서비스의 제공 사이에 '관련성'(connection)이 필요하다는 점을 고려하여야 하고, 이 때 직접적 및 간접적인 관계가 모두 관련이 있으며 고려되어야 한다.[73] 그러나 이러한 직접적 및 간접적 관계의 관련성에 관하여 가이드라인은 추가적인 설명을 하고 있지 않아서 이에 관한 명확한 설명이 필요하다. 특히 EU 역외 처리자의 경우 간접적 관계가 적용될 수 있는

71) 이와 관련하여 EDPB는 '계약 의무에 적용가능한 법에 관한 규칙 593/2008 (Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I))' 제6조에서, 준거법이 없는 경우에, 소비자의 거주지 국가를 '목표하는 활동'(directing activity)의 기준이, 계약에 적용가능한 법으로서 소비자의 거주지 법을 지정하는 데 고려된다고 설명하였다. 가이드라인 15쪽.

72) 가이드라인 15-16쪽.

73) 가이드라인 15쪽.

예가 설명되는 것이 바람직할 것이다.[74]

위에서 언급한 바와 같이 상기 여러 요소들은 단독으로는 EU 내 정보주체에게 상품 또는 서비스를 제공하는 컨트롤러의 의도에 대한 명확한 지표로서 충분하지 않을 수 있다.[75] 그러나 컨트롤러의 상업적 활동에 관련된 요소들을 결합했을 때 EU 내 정보주체를 목표로 하는 상품 또는 서비스의 제공으로 함께 고려될 수 있는지 판단하기 위해서, 이들 요소는 각각 구체적으로(*in concreto*) 분석에서 고려되어야 한다.[76] 그러나, 단지 EU 내에서 컨트롤러나 프로세서 또는 중개자의 웹사이트에 접속할 수 있거나, 이메일이나 지리적 주소를 웹사이트에서 언급하거나, 국제통화코드 없이 전화번호를 언급하는 것만으로는, 그 자체로 EU 내에 소재하는 정보주체에게 상품 또는 서비스를 제공할 컨트롤러 또는 프로세서의 의도를 입증하기에는 충분하지 않다.[77]

3. 정보주체의 행동에 대한 감시

GDPR의 역외적용을 발동시키는 두 번째 유형의 활동은 EU 내에서 이루어지는 정보주체의 행동에 대한 감시이다. EU 내에 설립되지 않은 컨트롤러 또는 프로세서에 의한 EU 내 정보주체의 개인정보의 처리는, 그러한 처리가 EU 내에서 이루어지는 정보주체의 행동을 감시하는 것과 관련된 경우, GDPR의 적용대상이 된다.[78] 이렇게 GDPR의 적용을 개시하기 위해서는, 감시된 행동이 우선 EU 내 정보주체와 관련되어야 하고, 누적적 기준으로서 감시된 행동이 EU 영토 내에서 이루어져야 한다. 처리활동이 정보주체의 행동을 감시한다고 간주될 수 있는지 판단하기 위해서는, 자연인이 인터넷상에서 추적되고 있는지가 확인되어야 한다. 이러한 활동은 특히 자연인과 관련된 결정을 위해서 또는 자연인의 개인적 선호, 행동 및 태도를 분석하거나 예측하기 위해서, 자연인을 프로파일링하는 개인정보처리기술의 잠재적 추후 사용을 포함한다.[79] 처리 활동이 행동 감시에 해당하는지 판단하는 데에는, 인터넷상에서 개인의 추적을 통하여 행동을 감시하는 경우뿐만 아니라, 개인정보 처리를 포함하는 다른 유형의 네트워크나 기술을 통한 추적, 예컨대 웨어러블이나 기타 스

74) AmCham EU, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3): Our Position*, p. 4 (2019.1.18.)
75) 가이드라인 15쪽, 각주 67의 본문 참조.
76) 가이드라인 16쪽.
77) GDPR 상설 제23항.
78) GDPR 상설 제24항.
79) GDPR 상설 제24항.

마트 디바이스를 통한 경우도 고려하여야 한다.[80]

컨트롤러 또는 프로세서 측면에서 감시 활동이 처리 활동에 대한 GDPR의 적용을 발동시키는지 판단할 때 '표적의 의도'(intention to target)의 필요한 정도를 규정하지 않는다. 그러나 '감시'라는 단어 사용은, 컨트롤러가 EU 내 개인의 활동에 대하여 관련 데이터 수집 및 추후 재사용을 위해 특정한 목적을 염두에 두고 있음을 암시한다.[81] 따라서, EU 내 개인의 모든 온라인 개인정보 수집 또는 분석이 자동으로 감시로 간주되는 것은 아니다.[82] 이 때 컨트롤러의 개인정보 처리 목적과, 특히 개인정보를 포함하는 추후의 행동 분석 또는 프로파일링 기술을 고려하는 것이 필요하다.

컨트롤러나 프로세서의 개인정보 처리가 정보주체의 행동 감시를 포함하는지 판단에 있어서 프로파일링 기술의 잠재적인 추후 이용을 포함하여 인터넷상 자연인의 추적이 핵심적 고려사항이 된다.[83] 따라서 행태 관련 광고(behavioural advertisement), 마케팅 목적의 지리적 기반(geo-localization) 활동, 쿠키 또는 지문과 같은 추적기술을 이용한 온라인 추적, 맞춤형 다이어트 및 온라인 건강 분석 서비스, CCTV, 개인 프로파일에 기초한 시장 설문조사 및 기타 행동 관련 연구, 개인의 건강상태에 관한 모니터링 또는 정기적 보고와 같이 컨트롤러 또는 프로세서의 광범위한 감시 활동을 포함하게 된다.[84] 한편 EU에 특정적인 결과를 포함한 세계적인 고객들의 행태를 분석하는 경우에 감시 개념의 해석이 필요할 것이다. 즉, 전세계 고객들의 행태를 분석하는 전략적 의사결정 과정에서의 EU 내 정보주체에 대한 감시는 GDPR의 역외적용을 발동하지 않는지 확인될 필요가 있다.[85]

Ⅳ. 국제법상 EU 회원국 법이 적용되는 장소에서의 처리

EU 내에 설립되지 않은 컨트롤러에 의한 개인정보 처리가, 국제법상 EU회원국의 법이 적용되는 곳에서 이루어진 경우에는, 해당 개인정보 처리에 GDPR이 적용된다.[86] 국제법상 EU회원국 법이 적용되는 경우에는 EU 내에 설립되지 않은 컨트롤

80) 가이드라인 17-18쪽.
81) 가이드라인 18쪽.
82) 가이드라인 18쪽.
83) GDPR 상설 제24항.
84) 가이드라인 18쪽.
85) AmCham EU, *sura note* 74.
86) 제3조 제3항.

러, 예컨대 회원국의 외교공관 또는 영사관 등에도 GDPR이 적용된다.[87] 외교공관 및 영사관의 정의와 지위는 '1961년 외교관계에 관한 비엔나협약'과 '1963년 영사관계에 관한 비엔나협약'에 규정되어 있다.

이렇게 EU회원국의 대사관과 영사관 등에서 수행된 개인정보 처리가 GDPR 제2조에 정의된 물적 적용범위에 속하는 경우, 그러한 처리에 GDPR이 적용됨을 명시한 것이다.[88] 이 경우 EU회원국의 외교공관 또는 영사관은 개인정보 처리의 컨트롤러 또는 프로세서로서, 정보주체의 권리, 컨트롤러와 프로세서에 관한 일반 의무, 개인정보의 제3국 또는 국제기구에의 이전 등 GDPR의 모든 관련 조항의 적용을 받는다. 예컨대, 한국에 소재하는 네덜란드 대사관이, 행정 지원을 위한 현지 직원을 채용하기 위해 온라인 접수절차를 개시한 경우, 한국 소재 네덜란드 대사관은 EU에 설립된 것은 아니지만, 국제법상 EU회원국 법이 적용되는 EU 국가의 외교공관이라는 점에서, 그의 개인정보 처리에 GDPR이 적용된다.[89] 또한, 공해상에서 여행 중인 독일 크루즈 선박이 맞춤형 선상 엔터테인먼트를 제공하기 위해 승선 중인 승객의 개인정보를 처리하는 경우, 이 선박은 EU 역외 공해상에 소재하고 있지만 독일에 등록된 선박이므로, 국제법상 그 개인정보 처리에 GDPR이 적용되는 것이다.[90]

V. EU에 설립되지 않은 컨트롤러 또는 프로세서의 대리인

GDPR 제3조 제2항에 따라 GDPR의 적용을 받는, 즉 GDPR의 역외 적용을 받는 컨트롤러 또는 프로세서는 EU에 대리인을 서면으로 지정하여야 한다.[91] 대리인(representative)은 GDPR 제27조에 따라 컨트롤러 또는 프로세서에 의하여 서면으로 지정되어 GDPR에 따른 그들 각자의 의무에 관하여 그 컨트롤러 또는 프로세서를 대리하는 EU에 설립된 자연인 또는 법인을 의미한다.[92] 대리인은 GDPR 제3조 제2항에 따라 GDPR의 역외 적용을 받는 EU 역외 컨트롤러 또는 프로세서에 대

87) GDPR 상설 제25항.

88) GDPR은 전체적 또는 부분적으로 자동화된 수단에 의한 개인정보 처리에 적용된다. 또한 개인정보가 파일링시스템을 구성하거나, 이를 구성할 의도로 처리되는 경우에는 수동적 개인정보 처리에도 적용된다. GDPR 제2조. GDPR의 물적 적용범위에 관해서는 박노형 외, EU 개인정보보호법 -GDPR을 중심으로-, 박영사, 2017, 8-9쪽 참조.

89) 가이드라인 19쪽.

90) 가이드라인 19쪽.

91) GDPR 제27조 제1항.

92) GDPR 제4조 제17호.

한 GDPR의 집행을 보장할 목적으로 도입된 개념이다.[93]

1995년 EC지침도 대리인에 관하여 유사한 의무를 부과하고 있었다. 개인정보 처리 목적으로 회원국 영토에 소재한 '처리 수단의 이용'을 하지만 공동체 영토에 설립되지 않은 컨트롤러는, 동 지침에 따라 공동체 내에 대리인을 지정하도록 요구되었다.[94] GDPR은 대리인의 지정에 관한 제27조 제2항의 예외가 적용되지 않는 경우, 제3조 제2항에 따라 역외 적용을 받는 컨트롤러는 물론 프로세서도 대리인을 지정하도록 요구한다. 이렇게 EU에 지정된 대리인의 실재는 GDPR 제3조 제1항에서 규정된 컨트롤러나 프로세서의 사업장이 아닌 점에 유의하여야 한다.[95] 다만, 대리인의 지정에 관하여, 동 가이드라인은 '대리'(represent)라는 용어가 대리인이 EU 역외 컨트롤러나 프로세서를 대리하는 '위임장'(power of attorney)을 수령해야 하는 것으로 의미하는지 분명하게 밝히고 있지 않다.[96] 해당 위임장이 요구되는 경우라면 대리인의 위임장 범위가 명확하지 않고, 위임장이 요구되지 않는다면 대리인이 단순히 '의사전달자'(communicating messenger)로서 활동하는 역할에만 그치는 것인지도 분명하지 않다.

1. 대리인의 지정

컨트롤러 또는 프로세서는 GDPR에 따른 자신의 의무에 관하여 자신을 대신하여 행동하도록, '서면 지시'(written mandate)에 의하여 명시적으로 대리인을 지정하여야 한다.[97] 이러한 서면 지시는 EU 역외 컨트롤러나 프로세서와 EU 역내 대리인 사이의 관계를 규율한다. 이러한 대리인의 지정은 컨트롤러나 프로세서의 GDPR에 따른 '책임이나 법적 책임'(responsibility or liability)에 영향을 주지 않는다.[98] 이러한 대리인의 직무는 GDPR의 준수를 보장하기 위하여 취해진 행동에 관하여 소관 감독당국과의 협력을 포함한다.[99]

실제로 대리인의 기능은 '서비스 계약'에 따르고, 이러한 대리인은 EU에 설립된

93) 가이드라인 23쪽.
94) EC지침 제4조 제2항.
95) 가이드라인 20쪽.
96) Baker McKenzie, *Guidelines on the Territorial Scope of the GDPR (Art. 3) and on Representatives (Art. 27)*, (2018.12.12.).
97) GDPR 상설 제80항.
98) GDPR 상설 제80항.
99) GDPR 상설 제80항.

법무법인, 자문회사, 민간기업 등 다양한 범위의 상업적 및 비상업적 실체가 될 수 있다.[100] 하나의 대리인은 EU 역외 여러 컨트롤러와 프로세서를 위하여 활동할 수 있다.[101] 기업 등이 대리인의 역할을 수행할 때는, 대리하는 각각의 컨트롤러 또는 프로세서에 대하여 책임을 지는 한 명의 개인을 주된 연락처로서 지정하고 해당 서비스 계약에 기재하도록 권고된다.[102]

컨트롤러나 그의 대리인이 감독당국에게 대리인의 지정을 통고해야 할 의무는 명시적이지 않다. 그러나, 정보제공 의무에 관한 GDPR 제13조 제1(a)항과 제14조 제1(a)항에 따라 컨트롤러는 정보주체에게 EU 내 대리인의 신원에 관한 정보를 제공하여야 한다. 이러한 정보는 컨트롤러의 프라이버시 통지에 포함되거나 개인정보의 수집 당시 정보주체에게 제공되는 공개 정보가 되어야 한다. EU 역외 컨트롤러가 GDPR 제3조 제2항에 따라 GDPR의 역외 적용을 받는 경우 EU 내 정보주체에게 자신의 대리인의 신원을 고지하지 않으면 GDPR의 투명성 의무를 위반하게 된다.[103] 또한, 대리인에 관한 정보는 소관 감독당국과의 협력관계에 따른 연락을 위하여 감독당국이 쉽게 접근할 수 있어야 한다.[104]

예컨대, 한국에 소재하고 관리되는 웹사이트가 영어, 프랑스어, 네덜란드어 및 독일어로 이용 가능하고 유로나 파운드로 결제되도록 맞춤형 가족사진 앨범의 편집, 출력 및 배송 서비스를 제공하는 경우, 이 웹사이트가 해당 앨범을 우편으로 영국, 프랑스, 벨기에, 네덜란드, 룩셈부르크 및 독일에서만 배달되는 것을 나타내면, 이 웹사이트는 GDPR 제3조 제2(a)항에 따라 GDPR의 적용을 받게 된다. 이 경우 해당 컨트롤러는 EU에 대리인을 지정하여야 하는데, 대리인은 영국, 프랑스, 벨기에, 네덜란드, 룩셈부르크, 또는 독일의 한 회원국에 설립되어야 한다.[105]

EDPB는 EU 내 대리인의 기능이 EU 역내에 설립될 외부의 개인정보보호책임자(data protection officer: DPO)의 임무와 양립하는 것으로 고려하지 않는다.[106] 컨트롤러나 프로세서는 DPO가 자신의 직무 수행에 관하여 어떠한 지시도 받지 않도록 보장하여야 하기 때문이다.[107] 특히 DPO는 자신이 컨트롤러의 직원인지 여부

100) 가이드라인 20쪽.
101) 가이드라인 20쪽.
102) 가이드라인 20쪽.
103) 가이드라인 21쪽.
104) 가이드라인 21쪽.
105) 가이드라인 21쪽.
106) 가이드라인, 20쪽.
107) GDPR 제38조 제3항.

에 관계없이 독립된 방식으로 자신의 의무와 직무를 수행할 지위에 있어야 한다.[108] 이렇게 독립성과 자율성을 가지는 DPO는 컨트롤러 또는 프로세서의 직접적인 지시를 받아야 하는 대리인과 양립할 수 없다.[109] 또한, EDPB는 EU 내 컨트롤러의 대리인 기능이 동일한 컨트롤러에 대한 프로세서 기능과도 양립하는 것으로 고려하지 않는다.[110]

2. 대리인 지정 의무의 면제

EU 역외 컨트롤러 또는 프로세서의 EU 내 대리인 지정의 의무는 다음의 두 가지 경우 면제된다. 첫째, 개인정보 처리의 성격, 문맥, 범위와 목적을 고려하여 처리가 간헐적이고, 대규모로 제9조 제1항에 언급된 특수한 범주의 개인정보의 처리[111] 또는 제10조에 언급된 범죄경력 및 범죄행위에 관련된 개인정보의 처리를 포함하지 않고, 자연인의 권리와 자유에 대한 위험을 초래할 것 같지 않은 경우이다.[112] 여기서 대규모의 처리가 정의되지 않지만, DPO에 관하여 대규모의 처리를 결정할 때 고려되는 다음의 요소가 고려될 수 있을 것이다: 구체적 수 또는 관련 인구의 비율로서 해당 정보주체의 수, 처리되는 데이터의 양 및/또는 다른 데이터 항목의 범위, 개인정보 처리 활동의 기간 또는 상시성, 처리 활동의 지리적 범위.[113] 둘째, 공공당국 또는 기관이 개인정보를 처리하는 경우에도 대리인의 지정 의무가 면제된다.[114]

3. 정보주체가 소재하는 회원국들 중 하나에 설립

대리인은 정보주체가 소재하고, 상품 또는 서비스가 그에게의 제공과 관련하여 개

108) GDPR 상설 제97항 및 Article 29 Data Protection Working Group, *Guidelines on Data Protection Officers ('DPOs')*, p. 15 (2016년 12월 13일 채택, 2017년 4월 5일 개정, 이하 'WP 243 rev.01'이라 함) 참조.

109) 그러나, EU 내 대리인으로서 활동하는 외부 DPO는 자신이 GDPR에 부합하지 않는다고 판단한 컨트롤러나 프로세서의 결정이나 조치를 정보주체에게 전달하도록 지시를 받을 수 있다. 가이드라인 제21쪽, 각주 25.

110) 가이드라인, 21쪽.

111) 특수한 범주의 개인정보는 인종이나 민족적 기원, 정치적 견해, 종교적 신념, 유전정보, 건강정보 등, 그 성질상, 처리되는 경우 정보주체에게 위험을 야기할 수 있어서 특별한 보호를 필요로 하는 개인정보이다. GDPR 제9조 참조.

112) GDPR 제27조 제2(a)항.

113) WP 243 rev.01, p. 8.

114) GDPR 제27조 제2(b)항.

인정보가 처리되거나 그의 행동이 감시되는 회원국들 중 하나에 설립되어야 한다.[115] 개인정보가 처리되는 정보주체들의 상당한 비율이 특정 회원국에 소재하는 경우, 대리인은 그 회원국에 설립되면 되겠지만, EDPB는 대리인이 설립되지 않고 서비스나 상품이 제공되거나 행태가 감시되는 회원국들의 정보주체도 대리인에게 용이하게 접근 가능할 것을 권고한다.[116] EU 내 대리인의 설립 기준은 개인정보가 처리되는 정보주체들의 소재인데, 다른 회원국에 설립된 프로세서에 의한 처리 장소는 대리인 설립의 소재의 결정에 대한 적절한 요소가 될 수 없다.[117]

예컨대, EU에 사업 실재나 사업장을 가지지 않지만 GDPR 제3조 제2항에 따라 GDPR의 역외 적용을 받는 한국의 제약회사가 벨기에, 네덜란드 및 룩셈부르크의 병원들이 수행하는 임상시험을 지원하는데 동 임상시험에 참여하는 환자들 다수는 벨기에에 소재한다. 컨트롤러인 한국의 제약회사는 동 임상시험에 참여하는 환자들인 정보주체가 소재하는 이들 세 회원국들 중의 하나에 설립되는 대리인을 지정해야 한다. 환자들 대부분이 벨기에에 거주하는 점에서 동 대리인은 벨기에에 설립되겠지만, 벨기에에 설립된 대리인은 네덜란드와 룩셈부르크의 정보주체들과 감독당국들에게도 용이하게 접근 가능하도록 해야 한다.[118]

4. 대리인의 의무와 책임

EU 내 대리인은 자신이 대리하는 컨트롤러 또는 프로세서의 GDPR의 의무에 관하여 이들 각각을 위하여 행동하면서, 다음의 의무와 책임을 진다. 정보 제공에 관한 GDPR 제13조와 제14조에 따라 정보주체에게 대리인의 신원과 연락정보가 제공되어야 하는데, 대리인은 자신이 대리하는 컨트롤러 또는 프로세서와 정보주체 사이의 연락을 원활하게 하여야 한다. 컨트롤러 또는 프로세서의 대리인은 이들의 책임 아래 처리 활동의 기록을 유지하여야 한다.[119] 이러한 기록의 유지는 '공동의 의무'(joint obligation)가 되고, EU에 설립되지 않은 컨트롤러 또는 프로세서는 자신의 대리인에게 모든 정확하고 최신의 정보를 제공하여서 대리인이 기록을 유지하고 이

115) GDPR 제27조 제3항.
116) 가이드라인 22쪽.
117) 가이드라인 22쪽.
118) 가이드라인 22쪽. 이 사례에서 임상시험에 관한 EU 규칙 536/2014 (Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC)의 제74조가 적용될 수 있다.
119) GDPR 제30조.

용가능하게 하여야 한다.[120]

대리인은 컨트롤러 또는 프로세서에게서 받은 지시에 따라 자신의 직무를 수행하는데, 이러한 직무에는 GDPR의 준수를 보장하기 위하여 취해진 조치에 관하여 소관 감독당국과의 협력을 포함한다.[121] 따라서, 감독당국은 EU 역외 컨트롤러 또는 프로세서의 의무 준수에 관련된 사안에 관하여 대리인을 접촉할 것이고, 대리인은 요청 감독당국과 EU 역외 컨트롤러 또는 프로세서와 정보 또는 절차적 교환을 원활하게 하여야 한다.[122] 따라서 이러한 연락은 소관 감독당국과 해당 정보주체들이 이용하는 언어에 의하여야 한다.[123]

EU 내 대리인의 지정으로 GDPR에 따른 컨트롤러 또는 프로세서의 '책임과 법적 책임'(responsibility and liability)은 영향을 받지 않고, 컨트롤러 또는 프로세서 자신에게 개시될 수 있는 법적 조치도 영향을 받지 않는다.[124] 따라서, 컨트롤러 또는 프로세서에 대하여 동일한 방식으로 대리인에게 집행조치가 개시될 수 있다. 대리인의 법적 책임을 위하여 과징금과 벌칙이 대리인에게 부과될 수 있다.[125]

VI. 결 론

EU GDPR의 역외 적용은 EU의 새로운 개인정보보호 프레임워크의 가장 혁신적인 내용이면서, 실제로 가장 어려운 쟁점이 되고 있다. GDPR의 역외 적용을 포함하여, 영토적 적용 범위에 관한 EDPB의 가이드라인은 영토적 적용 범위에 관한 해석에서 중요한 지침이 된다. 그러나, 가이드라인의 설명에 의해서도 아직 해결되지 않은 쟁점들이 있다. 예컨대, EU 역외 소재 컨트롤러가 EU 내 프로세서를 이용하는 경우, EU 내 프로세서는 마땅히 GDPR의 의무를 이행하도록 요구되는데, 개인정보의 국외 이전과 관련하여 프로세서가 EU 역외 소재 컨트롤러에게 개인정보를 이전하는 경우 프로세서가 GDPR 준수와 관련하여 어떠한 의무를 어떻게 이행하는지에 대한 설명이 필요하다. EU 내 프로세서가 처리한 개인정보를 EU 역외 컨트롤러에게 다시 이전할 수 있게 하는 법적인 장치가 명확하지 않기 때문이

120) 가이드라인 23쪽.
121) GDPR 상설 제80항.
122) 가이드라인 23쪽.
123) WP 243 rev.01, p. 10.
124) GDPR 제27조 제5항 및 상설 제80항 참조.
125) 가이드라인 23쪽.

다.[126] 또한 EU 역외의 모기업이 EU 내 자회사의 피고용인 개인정보를 수령하는 경우에는, 동 자회사가 EU 역외 모기업의 사업장(establishment)이 되는 것인지, 그리고 EU 역외 모기업이 EU 내 피고용인에게 혜택을 제공하는 경우 GDPR 제3조 제2(a)항에 따라 GDPR의 역외 적용을 받게 되는지도 분명하지 않다.[127] 한편, EDPB의 가이드라인이 GDPR의 역외적용에 관하여 구체적인 상황을 들어 설명하는 것은 이러한 경우에 해당하는 EU 역외기업에게 긍정적인데, 이러한 사례의 설명에서 1995년 EC지침의 적용 사례를 GDPR의 보다 강화된 규정의 적용 사례로서 설명하는 것은 자칫 잘못된 설명이 될 수 있고, 이러한 사례를 통한 설명도 충분하지 않을 수 있다. 예컨대, EU 역외 모기업과 EU 역내외 자회사들로 구성된 기업집단에서 EU 역외 실체에게 GDPR이 적용되지 않는 경우, EU 역외 모기업에 대한 설명이 필요할 것이다. EU 역외 모기업이 EU 내에 사업장을 보유하는 사실만으로 동 모기업의 주주들과 투자자들의 개인정보 처리에 자동적으로 GDPR이 적용되는 것은 아니기 때문이다.[128]

GDPR의 영토적 적용 범위는 1995년 지침과 달리 역외 적용의 범위를 대폭 확대되었다. 따라서 한국에 설립된 기업도 GDPR의 적용을 받을 수 있다. GDPR의 영토적 적용 범위의 해석과 적용은 특히 한국 등 EU 역외에 설립된 기업 등에게 실무적으로 어려운 문제가 되고 있다. 한국기업이 EU에 소재하는 정보주체에게 상품이나 서비스를 제공하는 경우 등에서 정보주체의 개인정보를 처리하는 활동에 관하여 GDPR의 적용을 받는지 확인하고, GDPR의 적용을 받아야 하는 경우 GDPR의 관련 규정을 위반하여 제재 등의 불이익을 받지 않아야 할 것이다. 이 점에서 GDPR의 관련 규정의 본문은 물론 상설과 특히 영토적 적용 범위에 관한 EDPB의 가이드라인에 대한 올바른 이해가 요구된다.

126) Eduardo Ustaran, "EDPB's common sense approach to the GDPR's territorial scope", IAPP (2018.11.26.).

127) Baker Mckenzie, *supra note* 96.

128) AmCham EU, *sura note* 74.

참고문헌

I. 국내문헌

박노형 외 8인, EU 개인정보보호법 -GDPR을 중심으로-, 박영사, 2017.

II. 외국문헌

White & Case, Unlocking the EU General Data Protection Regulation, 2017.

AmCham EU, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3): Our Position, p. 4 (2019.1.18.)

Baker McKenzie, Guidelines on the Territorial Scope of the GDPR (Art. 3) and on Representatives (Art. 27), (2018.12.12.)

Eduardo Ustaran, "EDPB's common sense approach to the GDPR's territorial scope", IAPP (2018.11.26.)

European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR(Article 3) - Version for public consultation (2018.11.16)

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP169 (2010.2.16)

Article 29 Data Protection Working Party, Update of Opinion 8/2010 on applicable law in light of the CJEU judgment in Google Spain, WP179 update (2015.12.16)

Article 29 Data Protection Working Party, Guidelines for identifying a controller or processor's lead supervisory authority, WP 244 rev.01 (2016.12.13. 채택, 2017.4.5 개정)

Article 29 Data Protection Working Group, Guidelines on Data Protection Officers ('DPOs') (2016.12.13. 채택, 2017.4.5 개정)

Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság (C-230/14, 2015.10.1)

Verein für Konsumenteninformation v. Amazon EU Sarl, (C-191/15, 2016.7.28)

Google Spain SL, Google Inc. v AEPD, Mario Costeja González (C-131/12, 2014.5.13)

Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller, Judgment of the Court (Grand Chamber) (2010.12.7)

Peter Pammer v Reederei Karl Schlüter GmbH & Co KG (C-585/08) and Hotel Alpenhof GesmbH v Oliver Heller (C-144/09) (Joined cases C-585/08 and C-144/09)

Bond van Adverteerders and Others vs. The Netherlands State, CJEU, C-352/85 (1988. 4.26.)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services

Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations

Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC)

논문 투고일: 2019. 04. 30.
심사 완료일: 2019. 05. 31.
게재 확정일: 2019. 06. 11.

[Abstract]

A Review of the Territorial Scope of the EU GDPR

Nohyoung Park* · Myung-Hyun Chung**

The General Data Protection Regulation (GDPR), which started to apply on 25 May 2018, is the general law on data protection of the European Union (EU). The GDPR applies, according to the territorial sovereignty under international law, to those controllers and processors within the EU. However, It applies also to those certain controllers and processors even not established in the EU for the data protection of the data subjects in the EU. That means that those companies not established in the EU, which are involved in data processing, should abide by the GDPR in the case where the EU is affected in respect of such data processing. Contrary to the 1995 Directive of the European Community, replaced by the GDPR, the territorial scope of the GDPR extends to, beyond those controllers making use of equipment, automated or otherwise, situated on the territory of the EU, those controllers or processors not established in the EU, 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 EU. In order to clarify the rules on the territorial scope of the GDPR, the European Data Protection Board (EDPB) adopted the Guidelines 3/2018 on the territorial scope of the GDPR on 16 November 2018.

The extension of the territorial scope of the GDPR may be understood, in the context of the world-wide increasing data flows, for the comprehensive protection of the data subjects in the EU and for providing for a level-playing field to those companies operating in the EU. Though, the extended extraterritorial application of the GDPR is certainly one of the most innovative provisions of the GDPR and is also one of the most difficult matters in its application. Even Korean companies, not established in the EU, should pay attention to the GDPR in their business by understanding the GDPR provisions and preparing for their correct observance, if found to be extra-territorially applied, so as not to risk any sanctions provided in the GDPR. In this respect, Korean companies should rightly understand the provisions of the text of the GDPR, its recitals, and the guidelines of the EDPB.

Key Words: EU, data protection law, GDPR, territorial scope, extraterritorial application, representative

* Professor, Korea University School of Law(Lead author)

** Lecturer, Korea University School of Law(Corresponding author)