

EU 개인정보보호 적정성 평가의 주요내용과 시사점

박미사 허해녕* 김 원**
 한국인터넷진흥원 주임연구원
 한국인터넷진흥원 팀장 *
 한국인터넷진흥원 본부장 **

I. 배경

1. EU 개인정보보호지침

유럽연합(EU)은 1995년부터 회원국 시민의 개인정보보호를 위해 EU 개인정보보호지침(EU DIRECTIVE 95/46/EC)을 제정하여 시행하고 있다. 동 지침의 제 4 장에서는 개인정보의 국외이전에 대해 규정하고 있으며, EU 회원국에서 비회원국으로 개인정보를 이전하는 경우 원칙적으로 그 비회원국이 적정한(Adequate) 수준의 개인정보보호를 보장할 경우에만 이전이 가능하도록 규정하고 있다[5].

동 지침 제 25 조 제 1 항은 EU 회원국이 개인정보를 제 3 국으로 전송하는 경우에 대해 제 3 국이 “적정한 수준의 보호(Adequate level of protection)”를 보장하는 경우에 한해 가능하도록 규정하고 있으며, 제 2 항에서는 제 3 국에 의한 보호의 적정 수준은 하나의 정보이전 작업 또는 일련의 정보이전 작업을 둘러싼 모든 상황을 고려하여 평가해야 한다는 점을 규정하고 있다. 특히, 정보의 성질, 예정되어 있는 처리 작업의 목적과 기간, 정보 송신국과 최종 수신국, 당해 제 3 국에서 유효하게 시행되는 일반적·분야별 법규범, 제 3 국에서 시행되는 전문적 법규범과 보안 조치를 고려하도록 한다고 규정하고 있다.

동 지침 제 26 조는 적절한 수준의 보호를 보장하지 않는 제 3 국으로 개인정보의 이전 또는 전송에 대한 예외 상황을 규정한다. ① 데이터 주체가 이러한 전송에 대해 명백하게 동의를 한 경우, ② 데이터 주체와 컨트롤러 간의 계약 이행 또는 데이터 주체의 요청에 따라 취해진 사전 계약 조치의 이행을 위해 필요한 전송인 경우, ③ 계약자와 제 3 자 사이에 데이터 주체의

* 본 내용은 박미사 주임연구원(02-405-6496, ms2437@kisa.or.kr)에게 문의하시기 바랍니다.

** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

이익을 위해 체결된 계약의 체결 또는 이행에 필요한 경우, ④ 중요한 공익을 위해서 법적 요구 등을 위해 필요한 전송인 경우, ⑤ 데이터 주체의 중요한 이익을 보호하기 위해 이전이 필요한 경우, ⑥ 법률 또는 규칙에 따라 대중에게 정보를 제공하기 위해 등록부에 등록되어 있는 경우에 제 25 조 제 2 항이 의미하는 적절한 수준을 보장하지 않는 제 3 국으로 개인정보 이전이 가능하다.

[표 1] EU 개인정보보호지침의 국외이전 관련 주요 내용

구분		주요 내용
제 3 장 개인정보의 국외 이전	제 25 조 원칙	- 제 3 국이 “적정한 수준의 보호(Adequate level of protection)”를 보장하는 경우에 한하여 개인정보의 국외 전송 허용 - 제 3 국에 의한 보호의 적정 수준은 하나의 정보이전 작업 또는 일련의 정보이전 작업을 둘러싼 모든 상황을 고려하여 평가해야 함을 규정
	제 26 조 적용 예외	- 제 25 조의 원칙의 예외를 인정하는 것에 의하여 그리고 특정 사례를 규율하는 국내법의 다른 규정을 보호하기 위하여, 회원국은 제 25 조 제 2 항이 의미하는 보호의 적절한 수준을 보장하지 않는 제 3 국으로서의 일회의 혹은 일련의 개인 정보 이전을 가능하도록 하는 조건들을 규정하도록 명시

2. 개인정보보호 일반규정(GDPR)

EU 개인정보보호지침은 2018 년 5 월부터 시행되는 개인정보보호 일반규정(General Data Protection Regulation: GDPR)으로 대체된다. EU 개인정보보호지침은 회원국 국내에 직접 적용되는 것이 아니라 회원국 자체를 대상으로 하여 각 회원국이 국내입법을 할 때 준수해야 하는 기본적인 틀을 제시하는 것이라는 점에서 한계가 있고, 회원국에서 제정하는 별도의 국내법에 따라 다르게 시행될 수 있다. 이와 달리 규칙(Regulation) 형태로 제정된 GDPR 은 EU 차원에서 개인정보보호에 관한 일반법을 새롭게 마련하고자 하는 노력의 결과로 평가할 수 있다는 점에서 의의가 있다[4].

개인정보보호지침에서와 마찬가지로, GDPR 에서도 “적정한 보호 수준”을 보장하지 않는 경우 사업자가 EU 역외의 제 3 국으로 개인정보를 이전하는 것을 원칙적으로 금지한다(GDPR 제 44 조, 제 45 조). 또한, 기존의 개인정보보호지침 하에서 이루어진 적정성에 대한 판단은 GDPR 에서도 계속해서 적용되나, 4 년에 한 번씩 재검증을 받아야 한다.¹⁾

1) 개인정보보호 일반규정의 유럽의회안(案)에서는 기존 개인정보보호지침 하에서의 적정성 판단은 규정이 시행된 날로부터 5 년간 유효라는 조항이 있었으나 최종안에서는 삭제되었다.

[표 2] EU GDPR의 국외이전 관련 주요 내용

조항	주요 내용
제 44 조 이전(transfers)을 위한 통칙	- 현재 처리 중이거나 제 3 국 또는 국제기구로의 이전 후에 처리될 예정인 개인정보는 본 규정의 나머지 조문에 따라 정보처리자와 수탁처리자가 본 장에 규정된 조건을 준수하는 경우에만 이전이 가능하며, 여기에는 해당 제 3 국이나 국제기구로부터 기타 제 3 국이나 국제기구로 개인정보가 이전되는 경우도 포함
제 45 조 적정성 결정에 따른 이전(transfers)	- 적정성 결정에 따른 개인정보 이전 문제를 다루고 있음 - EU 집행위원회가 제 3 국, 해당 제 3 국의 영토나 하나 이상의 지정 부문, 또는 국제기구가 적절한 보호수준을 보장한다고 결정한 경우 제 3 국 또는 국제기구의 개인정보 이전이 가능하며, 이 경우 특별한 인가가 필요 없음 - 적정성을 평가할 때 EU 집행위원회가 고려해야 할 사항과 역할 등을 규정

<자료> <http://www.privacy-regulation.eu>

즉, GDPR은 개인정보의 국경 간 이전 문제를 규율하면서, 국외이전을 허용하는 근거로서 적정성 결정(Adequacy decision)을 제시하고, 적정성 결정이 없는 경우 적절한 안전조치(Appropriate safeguards)에 의한 이전을 규정한다.

3. EU-US 세이프 하버와 프라이버시 쉴드

미국은 EU의 개인정보보호 기준에 부합하기 위해 국내법을 정비하는 대신 분야별 규제와 자율규제에 위임해 온 기존의 개인정보보호제도를 유지하면서 새로운 개인정보보호의 기준을 마련하기 위해 2000년 7월 27일 미국과 EU 간 세이프 하버 협정(Safe Harbor)을 체결하였다. 세이프 하버 협정에 따라 미국 내의 단체나 관련기업들이 자발적으로 세이프 하버 원칙을 준수하겠다고 상무부에 신고할 경우, 충분한 개인정보 보호조치를 강구하고 있는 것으로 간주하여 EU로부터 정보 이전을 계속해서 받을 수 있다. 또한, 세이프 하버에의 가입은 의무가 아니라 가입을 희망하는 사업자와 단체의 자율적인 판단에 따라 결정하도록 하였다[4],[5].

그러나 EU 사법재판소가 2015년 10월 세이프 하버 무효화를 판결한 이후에는 프라이버시 쉴드(Privacy Shield) 체제로 전환되었다. EU 집행위원회가 2016년 7월 12일 미-EU 프라이버시 쉴드 협약을 공식 승인함으로써, 2015년 10월 세이프 하버 무효화 이후 이어져온 개인정보 전송 문제의 법적 불확실성이 해소되었다. 프라이버시 쉴드는 미국으로 전송된 EU 시민들의 개인정보에 대한 집단 감시를 방지할 새로운 안전장치들과 프라이버시 쉴드에 자기 인증으로 등록된 기업들의 의무사항에 대해 규정하고 있다.

미 상무부는 자국 기업들이 프라이버시 쉴드 프레임워크를 검토하고 2016년 8월 1일부터 자발적으로 프라이버시 쉴드 등록 인증에 참여하도록 독려했다. EU 측에서는 EU 집행위원회가

프라이버시 쉴드 협약과 관련한 법률문서들을 공개하고 EU 회원국 소비자들이 미국 기업의 개인정보 취급 방침에 대해 불만을 제기할 수 있는 절차에 대한 안내 자료를 제공했다. 프라이버시 쉴드에 등록된 기업들은 불필요한 개인정보를 삭제해야 하는 등의 새로운 의무 조건을 적용 받게 되며, 미 기업들의 개인정보보호 현황에 대한 지속적인 검토와 문제 해결을 위한 연례 합동 점검 절차도 마련되어 있다[3]. 특히, 제 3 자에게 개인정보를 재이전(Onward transfer)하는 요건을 엄격하게 했으며, EU 회원국 국민의 개인정보에 대한 미국 정보기관의 접근을 규율하기 위해 미 정부가 정보에 접근할 경우에 명확한 안전장치를 제공하고 투명성 의무를 이행할 것을 제시하였다[5].

II . EU 개인정보보호 적정성 평가

1. EU 개인정보보호 적정성 평가란?

‘EU 적정성 평가’는 역외국가가 EU 개인정보 보호지침의 요구 수준으로 개인정보가 보호되고 있는지를 평가하는 제도이다. ‘EU 적정성 평가’ 가입 국가의 기업들은 EU 기업들과 같이 EU 시민 개인정보를 국외로 이전하여 활용할 수 있다. 제 3 국의 적절한 보안 수준은 정보 이전 작업에 관련된 모든 상황에서 평가되며, 특히 정보의 성질과 제안된 처리기한, 정보 제공 국가, 법적 환경, 정보를 전송 받는 국가의 정보보호방침이나 정책 등이 중요한 고려대상이 된다[4].

[표 3] EU 개인정보보호지침(EU Data Protection Directive)의 내용

- ▶ OECD 개인정보보호 8 원칙 준수, 개인정보보호기구 설치·운영
- ▶ 적정한 수준(Adequate Level of Protection)으로 개인정보를 보호하지 않는 역외국가로의 개인정보 이전 제한
 - ※ 적정한 수준이란, ① OECD 가이드라인에 따른 개인정보 처리, ② 개인정보 침해 시 피해복구, ③ 독립적 개인정보보호 감독기구의 운영 등을 의미함
 - ※ 모든 EU 회원국(28 개)은 본 지침을 법제화하여 적용하고 있음

<자료> KISA

EU 개인정보보호지침 제 25 조 제 2 항은 적정한 수준의 평가가 개별 사례별로 이루어져야 함을 규정하며, 제 25 조 제 6 항은 특정 국가가 적정한 보호 조치를 취하고 있는지에 대해 EU 집행위원회가 결정할 수 있음을 규정하고 있다[2].

EU 의 적정성 평가 승인 시에는 해당 국가의 개인정보보호 관련 법령, 실질적인 법·제도 운영 현황 등을 종합적으로 고려한다. 개인정보 처리과정에서 법제도의 실효성, 피해구제 및 감독기관의 실체 등을 조사하기 위해 제 29 조에 따른 EU 각국 DPA 로 구성된 작업반을 운영하고 있다. 가입신청부터 최종 승인까지 2~10년 소요된다.

기존의 개인정보보호지침과 2018년 시행될 GDPR 이 “적정한 보호 수준(Adequate level of protection)”의 보장을 개인정보 역외이전의 기본 조건으로 삼고 있는 만큼 “적정한 보호 수준”의 의미에 대해 검토할 필요가 있다. 적정한 보호수준을 판단하기 위해서는 개인정보의 성격, 개인정보의 처리 목적과 기간, 개인정보의 최초 이전국과 최종 도착국, 제 3국에서 시행되고 있는 법률 규범·직무 규정 및 보안조치 등 개인정보 이전을 둘러싼 모든 환경이 고려되어야 한다[6].

‘EU 적정성 평가를 받은 국가(일명 Whitelist)’는 뉴질랜드를 비롯한 12개국으로, 이들 국가는 부가적인 안전조치 없이 28개 EU 회원국으로부터 개인정보 이전이 가능하다. 현재 국가 차원의 적정성 평가를 받지 않은 우리나라 기업은 역외이전 계약 체결²⁾ 후, 개별 회원국의 규제 심사를 거쳐야 개인정보의 국내 전송·처리가 가능하다. 이에 따라 개인정보 역외이전 계약체결 과정에서 28개 회원국별로 다른 규제 내용 준수를 위해 과도한 비용이 지출되고 비즈니스 프로

[표 4] EU 적정성 평가를 받은 국가 현황

국가	신청주체(승인일)	국가	신청주체(승인일)
뉴질랜드	EU 주재 뉴질랜드 대사관 (2009.12.)	안도라 (유럽 이베리아 반도)	EU 주재 안도라 대사관 (2010.10.19.)
우루과이	EU 주재 우루과이 대사관 (2008.10.)	페로 제도 (the Faroe Islands, 덴마크령 제도)	EU 주재 Faroese Islands 대사관 (2010.3.5.)
이스라엘	EU 주재 이스라엘 대사관 (2011.1.31.)	저지 (Jersey, 영국해협 영국령 섬)	EU 주재 Jersey 대사관 (2008.5.8.)
캐나다	EU 주재 캐나다 대사관 (부분 승인, 2001.12.20.)	맨 섬 (Isle of man, 잉글랜드와 북아 일랜드 사이에 위치한 섬)	EU 주재 Isle of Man 대사관 (2004.4.28.)
아르헨티나	EU 주재 아르헨티나 대사관 (2003.6.30.)	건지 (Guernsey, 영국해협 채널제도 섬)	EU 주재 Guernsey 대사관 (2003.11.21.)
스위스	EU 주재 스위스 대사관 (2000.7.26.)	-	-

<자료> KISA

2) “현지기업↔국내기업”, “지사↔본사” 간 고객정보, 지사 직원정보 등 역외이전 계약 체결

세스가 지연되는 문제가 발생한다. 국내 L 사의 경우 국외이전 계약 등으로 개별 국가(28 개)의 법률 적용 · 검토 비용이 약 38 억 원에 이르는 것으로 알려졌다.

2. EU 개인정보보호 적정성 평가 절차

EU 개인정보보호 적정성 평가는 ① 신청한 국가의 EU 의 적정성 기준 충족 여부를 자체평가(Self-assessment)하는 것으로 시작한다. ② EU 집행위원회는 적정성 평가 절차 진행 과정에서 신청이 거부되지 않도록 적정성 충족 여부에 대한 확실한 근거를 확인한다. 개인정보보호 적정성 평가를 신청한 국가는 EU 개인정보보호지침에 부합하도록 자국 개인정보보호법을 제정 및 시행할 수 있다. 또한, 개인정보보호지침 제 26 조 제 1 항에 의거해 개인정보보호 원칙의 예외 사유를 인정받을 수도 있다. EU 집행위원회가 적정성 요건을 충족한다고 판단한 후, ③ 29 조 작업반에 의견을 요청한다. ④ 29 조 작업반 내에서 EU 개인정보보호 감독기구(European Data Protection Supervisor: EDPS)와 각 회원국별 개인정보보호국(DPAs)의 의견이 수렴된다. 이 과정에서 다양한 사례별로 정보이전 실태 조사가 이루어지고 관계 전문가와의 면담 및 설문조사가 진행된다. 이를 근거로 ⑤ 최종 보고서가 작성되고, ⑥ 31 조 위원회에서 다수결에 따라 결정된다.

[표 5] 적정성 평가 세부 기준표

①단계	②단계	③단계	④단계	⑤단계	⑥단계
자체 평가	적정성 요건 충족 판단	29 조 작업반 의견 요청	회원국 의견수렴 및 Opinion 작성	최종 보고서 작성	최종결정 Decision (다수결)
신청국	EU 집행위	EU 집행위	29 조 작업반	EU 집행위	31 조 위원회

<자료> KISA

3. EU 개인정보보호 적정성 평가 기준

적정성 평가를 위해서는 평가 대상 국가에도 EU 와 본질적으로 동일한 수준의 개인정보보호 법규 등이 존재해야 한다. 개인정보에 적용할 수 있는 실질적인 보호 수단과 제 3 국에서 활용할 수 있는 개인정보보호 관련 감독 및 구제 조치라는 두 가지 측면 모두와 관련해서 해당국 시스템에 대한 포괄적인 평가가 이루어진다. 여기에는 법 집행 및 국가 보안 목적으로 공공기관이 개인 정보에 접근하는 것에 적용할 수 있는 제한 사항 및 안전장치에 대한 검토도 포함된다.

EU 집행위원회가 2017년 1월 공개한 보도자료에서는³⁾ 어떤 국가와 적정성 평가 관련 논의를 진행할 것인지 결정할 때 EU 집행위원회가 고려해야 할 네 가지 주요 기준이 제시되어 있다. 적정성 평가 대상을 선정하는 과정에서부터 기준이 적용되는 것이다. 첫째는 해당 제3국과 EU가 실질적으로 또는 잠재적으로 어느 정도 상업적인 관계를 맺고 있는가의 기준이다. 여기에는 자유무역협정 체결 여부 혹은 현재 진행 중인 무역 협상 등이 포함된다. 둘째는 EU로부터 개인정보가 이전되는 범위를 고려한다. 여기에는 지리적/문화적으로 얼마나 밀접한 관계인가가 반영된다. 셋째는 제3국이 속해 있는 해당 지역의 다른 국가들에 대해 개인정보 보호 분야에서 모범적인 역할을 하며 선구적인 역할을 수행할 수 있는가의 기준이다. 넷째는 해당 제3국과의 전반적인 정치적 관계, 특히 공동 가치의 증진과 국제 수준에서의 공동 목표 추구하고 관련한 부분을 평가해 대상을 선정한다.

이처럼 적정성 평가 대상국가가 결정된 후에는 실제 평가 원칙들이 적용된다. 29조 작업반의 실무작업보고서(working document)인 「EU 개인정보보호지침 제 25조 및 제 26조의 적용에 따른 제3국에 대한 개인정보의 이전(Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive)」에는⁴⁾ 개인정보보호 적정성 평가 기준을 ① 실체적 판단 기준, ② 절차적 판단 기준 등 두 가지 부문에서 제시하고 있다.

우선 실체적 판단 기준은 목적제한의 원칙 등 6개 기본원칙과 민간정보 처리제한 등 3개 추가원칙을 중심으로 법·제도의 실체적 측면을 확인하기 위한 것이다. 절차적 측면을 심사하기 위해서는 법·제도의 실효성 확보를 위한 집행기구, 감독시스템, 사법체계 등에 대한 원칙을 제시하고 있다. 또한, 국가기관에 의한 개인정보 접근·활용 제한 등 평가기준을 강화 중이다. 이 원칙들은 1980년의 OECD 가이드라인에서 정한 개인정보보호 8원칙을 반영하고 있다.

한편, EU 집행위원회는 EU 회원국으로부터 개인정보를 수탁하는 제3국의 정보보호 수준이 어느 정도인지 평가하는 데 효과적인 평가방법론(methodology)을 검토하기 위해 이를 위탁 연구한 바 있다. 벨기에의 정보와 법 연구소(CRID)가 EU 집행위원회에 제출한 연구 결과는⁵⁾ 29조 작업반의 실무작업보고서에 반영되었다.

3) "Digital Single Market-Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers", http://europa.eu/rapid/press-release_MEMO-17-15_en.htm

4) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf

5) "Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data: annex to the annual report 1998 (XV D/5047/98) of the working party established by Article 29 of Directive 95/46/EC"

[표 6] 29 조 작업반의 개인정보 보호 적정성 평가기준 내용

평가 기준		내용
기본 원칙	목적제한의 원칙	데이터는 특정한 목적에 따라 처리되고 목적 범위 내에서 이용·제공되어야 함
	정보의 질 확보 및 비례성 원칙	데이터는 정확해야 하고 필요한 경우 최신으로 업데이트되어야 함. 또한, 데이터는 이전 또는 처리되는 목적에 적합하고 관련성이 있어야 하며 목적에 비해 과도해서는 안 됨
	투명성 원칙	개인은 처리목적, 처리자 등 공정성을 위해 필요한 정보들을 투명하게 제공받아야 함
	안전성 원칙	개인정보처리자는 적절한 기술적·관리적 보안조치를 해야 함
	열람·정정 및 반대할 권리	정보주체는 처리 중인 자신에 관한 데이터의 사본을 받아볼 수 있고 부정확한 정보를 수정할 수 있으며, 자신에 관한 정보 처리를 반대할 권리를 가져야 함
	개인정보의 재이전 제한	일차적으로 개인정보를 제공받은 자가 다시 개인정보를 재이전하는 것은 재이전 받는 자가 적절한 보호수준을 보장하는 규칙의 적용을 받는 경우에만 허용됨
추가 원칙	민감정보 처리제한	민감한 정보로 분류되는 데이터는 정보 처리에 대한 정보주체의 명백한 동의 등 추가적인 안전조치를 확보해야 함
	다이렉트 마케팅 제한	데이터가 다이렉트 마케팅 목적으로 이전되는 경우, 정보주체는 opt-out 를 할 수 있어야 함
	개인에 대한 자동화된 결정 제한	자동 처리되는 개인정보 이전의 경우, 정보주체에게는 그러한 의사결정에 사용되는 로직을 알 권리가 있으며, 합법적인 이익을 보호하기 위한 추가적인 조치가 취해져야 함
절차적 기준	보호원칙이 잘 준수되는 체계의 확보	개인정보처리자가 자신들의 의무를 뚜렷이 인식하고, 정보 주체가 자신들의 권리 및 행사방법을 잘 알 수 있는 보호체계를 만들고, 효과적이고 역제력이 강한 제재수단을 통해 보호원칙을 확보
	정보주체의 권리행사를 지원하고 도와주는 보호체계	개인이 신속하고 효과적으로, 과도한 비용 부담 없이 자신들의 권리를 행사할 수 있어야 함. 이를 위해 민원·고충에 대한 독립적 조사가 보장되는 제도적 매커니즘
	보호원칙 미준수로 피해를 입은 자에 대한 적절한 구제조치 필요	손해배상이나 적절한 제재조치가 가능한 독립적 조정 또는 중재 시스템

<자료> KISA

III . EU 의 최근 동향

EU 집행위원회는 한국과 일본의 적정성 평가를 우선적으로 검토하겠다는 입장이다. 2017년 1월 10일 EU 집행위원회는 유럽 의회와 이사회에 보내는 “세계화된 세계에서의 개인 정보의 교환 및 보호(Exchanging and Protecting Personal Data in a Globalised World)”⁶⁾ 연락문서를 발표했으며, 이를 통해 EU 집행위원회가 2017년 한국과 일본을 시작으로 동아시아 및 동남아시아의

6) https://ec.europa.eu/newsroom/document.cfm?doc_id=41157

핵심 교역 파트너들과 적정성 결정에 관한 논의를 우선 진행할 것이라고 밝혔다. 또한, EU 는 각국 개인정보보호법의 현대화 진행 상황에 맞춰 인도와 중남미 국가들과도 협조할 계획임을 밝혔다¹⁾.

일본은 2014 년부터, 한국은 2015 년 10 월부터 정부차원에서 EU 집행위원회와 접촉을 시작했다. 현재 일본 정부는 적정성 평가와 관련하여 매우 적극적으로 EU 집행위원회와 협상을 추진 중이다. 일본은 “EU-日 FTA”와⁷⁾ “적정성 평가 가입”을 동시에 추진하고 있으며, 2017 년 3 월 20 일 브뤼셀에서 EU 집행위원과 일본 대표부(개인정보보호위원회·경제성 등) 면담이 이루어졌다. 일본은 적정성 평가의 조기 가입을 위한 EU 집행위원회와 일본 실무·고위급의 지속적 접촉을 추진하고 있다.

IV . 결론 및 시사점

EU 집행위원회는 2016 년 7 월 12 일 미-EU 프라이버시 쉴드 협약을 공식 승인하였으며, EU 는 2018 년 5 월 EU 의 단일화된 개인정보보호법인 개인정보보호 일반 규정(GDPR) 시행을 앞두고 있는 등 글로벌 개인정보 관련 법제도 환경이 변화하고 있다.

GDPR 에서는 기존의 개인정보보호 지침(EU Directive 95/36/EC)과 마찬가지로 개인정보의 국경 간 이전 문제를 규율하면서, “국외이전을 허용하는 근거로서 적정성 결정(Adequacy decision)을 제시하고, 적정성 결정이 없는 경우 적절한 안전조치(Appropriate safeguards)에 의한 이전을 규정”하고 있다.

이와 같이 EU 는 개인정보의 역외이전을 엄격히 규제하고 있어 그 동안 EU 진출 국내 기업들이 애로사항을 겪어 왔으며, 이에 대한 지원대책을 마련할 필요가 제기되었다. 이에 따라 우리나라는 EU 적정성 평가 가입을 위해 추진 중에 있으며, EU 집행위원회는 2017 년 1 월 10 일 한국과 일본의 적정성 평가를 우선적으로 검토하겠다는 입장을 발표한 바 있다.

우리나라가 EU 적정성 평가 가입국이 되면, 그 동안 한국 기업들이 EU 의 기업들과 거래할 때, 각 사안별로 규제 당국에 개인정보 보호조치에 대해 평가를 받았던 것을 면할 수 있게 된

7) 2017 년 3 월 21 일 일본 아베 총리는 EU-日 FTA 협상을 위해 EU 집행위원회를 방문하여 융커(Juncker) 집행위원장을 면담했다. 2016 년 11 월을 목표로 FTA 를 추진하였으나, 개인정보 국외이전 등의 이슈로 지연 중인 것으로 알려졌다.

다. 이렇게 될 경우, 역외이전 계약 등 추가 규제 없이 EU 기업과 동일한 조건에서 해외에서 영업 활동이 가능할 것으로 전망된다. 또한, EU 측과 거래하며 수집한 정보를 국외로 이전하는 것이 용이해지며, EU로 진출할 경우 규제 심사 등에 소요되는 비용과 시간을 절약할 수 있을 것으로 전망된다. 이로 인해 국내 기업의 EU 진출 여건이 개선되어 궁극적으로는 ICT 산업 발전에 기여할 것으로 예상된다. 또한, 국가적 차원에서는 개인정보보호 우수 국가로서 국가 이미지 제고 및 개인정보보호 규제 수준의 글로벌화를 달성할 수 있을 것이다.

[참고문헌]

- [1] EUROPEAN COMMISSION, “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL,” 2017. 1. 10(Digital Single Market–Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers 보도자료 포함).
- [2] EUROPEAN COMMISSION, “Working Party on the Protection of Individuals with regard to the Processing of Personal Data,” 1998. 7. 24.
- [3] TechCrunch, EU-US Privacy Shield open for sign ups from today, 2016. 8. 1.
- [4] 김일환, “개인정보 국외이전에 대한 국제적 기준과 내용에 관한 고찰”, 「미국헌법연구」 제 24 권 제 1 호, 2013. 4.
- [5] 최경진, EU GDPR 의 분석 및 시사점, Naver Privacy White Paper, 2016, p.146.
- [6] 최승재, 진창환, “개인신용정보의 국외 이전 규제 현황 및 EU GDPR 국외 이전 제정 조항의 시사점”, 한국정보법학회 2016 년 5 월 사례연구 발표자료, 2016, p.6.
- [7] <http://www.privacy-regulation.eu>