논문 19-44-05-24 The Journal of Korean Institute of Communications and Information Sciences '19-05 Vol.44 No.05
https://doi.org/10.7840/kics.2019.44.5.983

EU 개인정보보호 적정성평가 이슈와 정책 대응 방안

박 효 주•, 양 진 홍°

Issues of Adequacy Decision of GDPR and Policy Responses

Hyo-ju Park•, Jin-hong Yang°

요 약

EU는 자국민의 개인정보보호 보호를 위한 일반개인정보보호규정(GDPR)을 발효하였으며, 역외 국가가 적정 수준의 개인정보 보호조치를 확보하고 있는지를 평가하기 위한 적정성결정(Adequacy Decision)을 시행하고 있다. 적정성 평가를 거치지 않을 경우 개별 기업이 EU에 진출할 때 규제심사 등에 소요되는 비용과 시간이 천문학적 수준이며, 통과할 경우 국제적 수준의 개인정보보호 위상 강화 및 우리 기업의 EU 진출 가속화를 기대할 수 있다. 그러나 한국은 이미 두 차례 부적격 결정을 받았다. 따라서 본 연구는 적정성 평가의 내용 및 평가절차를 검토하고, 일본과 한국의 추진 현황을 파악하며 진행상의 법률적, 정책적 주요 이슈들을 분석해 우리나라가 이를 통과하기 위한 정책적 시사점을 도출하고자 하였다. 그 결과, 1)개인정보보호 가이드라인 및 보조규정 제정 2)적정성 평가 범위의 재검토 3)범정부 차원의 추진체계 구성 및 추진 과정의 투명성 확보 4)개인정보보호위원회의 실질적 독립성 확보가 우선 과제로 제시되었다. 향후 정부가 중장기적 시각으로 관련 법규 및 제도를 개정하고 EU협의회와 적극적인 협상을 이어나간다면 좋은 결과를 기대할 수 있을 것이다.

Key Words : GDPR, Adequacy Decision, Privacy Policy, Privacy Shield, Data Transfer

ABSTRACT

The EU has enacted the General Data Privacy Policy (GDPR) to protect the privacy of its citizens and has implemented an Adequacy Decision to assess whether the foreign country has adequate privacy protection measures. However, Korea has already been twice ineligible. The purpose of this study is to examine the content and evaluation procedure of the appropriateness evaluation, to grasp the current status of the promotion of Japan and Korea, and to analyze the legal and policy issues in order to draw policy implications for Korea to pass it. As a result, 1) Establishment of personal information protection guidelines and subsidiary regulations 2) Reexamination of scope of appropriateness evaluation 3) Establishment of transparency of constitution and process of government-wide level 4) Ensuring substantive independence of personal information protection committee as presented. If the government revise related laws and regulations in the mid- to long-term perspective and continues active negotiations with the EU Council, we can expect good results.

※ 이 논문은 2019 년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00261, IoT 환경에서 일반개인정보보호규정에 부합(GDPR Compliant)하는 개인정보 관리 기술 개발)
• First Author : Inje University Department of Computer Engineering, hjpark@inje.ac.kr, 정회원
° Corresponding Author : Inje University Department of Healthcare IT, jinhong@inje.ac.kr, 정회원
논문번호 : 201902-467-0-SE, Received February 14, 2019; Revised March 21, 2019; Accepted March 22, 2019

Ⅰ. 서 론

유럽연합(EU)은 자국민의 개인정보보호를 위해 개인정보보호 규제법인 GDPR(General Data Protection Regulation)을 발효하였다. GDPR은 기존의 가이드라인 성격을 가지던 유럽연합의 개인정보보호법과는 달리 각국에 실효 법으로 적용된다는 측면에서 차별성을 가지며, 2018년 5월 본격적으로 시행됨에 따라 EU 내 뿐 아니라 EU 시민들의 개인정보를 활용하여 서비스를 제공하는 해외 국가 및 기업들 에게도 큰 파장을 일으키고 있다.

그중에서도, GDPR은 개인정보의 역외이전, 즉 제3국으로의 전송과 관련해서 엄격한 규정(적절한 안전조치, appropriate safeguard)을 제시함에 따라 EU 시민들의 개인정보를 활용하여 서비스를 제공하고자 하는 EU 외 국가들의 기업에게 큰 영향을 미치고 있다. 이는 해당 조건을 충족하기 위한 과정이 까다롭고 시간과 비용 측면에서도 큰 노력이 필요하기 때문이다. EU에서는 이와 같은 불편함을 해소하기 위해 '적정성 평가'라는 제도를 두고 있다. 해당 평가를 통과한 국가에 한해서는 EU와 '동등한 수준'의 개인정보보호가 이루어진다고 판단, 추가 규제 없이 국가 간 개인정보의 자유로운 이전을 가능하게 하고 있다.

현재까지 적정성평가를 통과한 국가는 12개 국가이며, GDPR 관련 전반적인 사항을 총괄하는 EU내 위원회인 EU 집행위원회는 자체적인 기준에 따라 어떤 국가와 적정성 평가 관련 논의를 진행할 것인지를 결정하고 있다. 현재까지 적정성 평가를 통과한 아시아 국가는 전무 하였으며, 따라서 EU 집행위는 2017년 1월, 일본과 한국을 아시아 지역 우선 적정성평가 협상 선정 국으로 발표하였다. 일본의 경우 발 빠른 대응으로 인해 2018년 9월 5일 적정성 평가를 사실상 통과하였으며 2019년 1월 현재 행정적인 절차만 남겨두고 있는 상황이다. 그러나 우리나라는 이미 두 차례 부적격 통지를 받은 바 있어 적정성 평가를 통과하기 위한 다양한 노력을 기울이는 중이다.

적정성 평가는 GDPR 시행 후 국내기업이 개별적으로 사안에 따라 개인정보 이전 평가를 받기 위해 체결해야 하는 계약 및 EU 내 개별국가(28개국) 법률 적용 및 검토에 드는 천문학적 비용을 고려할 때 매우 중요도가 높은 사항이다. 예를 들어, 국내 L사의 경우 국외이전 계약 등으로 개별국가(28개)의 법률 적용 및 검토 비용이 약 38억 원에 이르는 것으로 알려졌다. 적정성 평가를 통과할 경우 EU지역에 진출한 국내기업이 현지 개인정보보호 규제에 따른 부담과 불이익 없이 영업 활동이 가능하게 되고 EU측과 거래하며 수집한 정보를 국외로 이전할 수 있으며, EU로 진출할 경우 규제심사 등에 소요되는 비용과 시간을 절약할 수 있게 된다. 또한, 국가적 차원에서 개인정보보호 우수 국가로서 국가 이미지 강화 및 규제 수준의 글로벌화를 달성할 수 있다. 따라서 본 논문에서는 GDPR의 개인정보 국외이전 관련 규정 및 적정성 평가의 내용에 대해서 검토하고, 먼저 적정성 평가를 통과한 일본의 전략 분석 및 국내 대응 현황 파악을 통해 향후 우리나라의 적정성평가 대응을 위한 정책적 시사점을 도출하고자 한다.

Ⅱ. EU 개인정보보호 적정성 평가

2.1 GDPR

GDPR은 EU 회원국 모두에게 법형식으로 규율되어 법적 구속력을 가지는 개인정보보호 일반법으로 우리나라의 개인정보보호법과 유사한 성격을 가진다. EU는 1995년부터 회원국 시민의 개인정보보호를 위해 EU 개인정보보호지침을 제정 및 시행했으나 각 회원국이 입법 시 참고하는 가이드라인의 성격이었으며 회원국에 직접 적용되는 것이 아니었다는 점에서 GDPR과 차이를 보인다[1].

GDPR은 EU환경 내에 데이터의 자유로운 흐름을 보장하고, 일관성 있는 규제 환경을 형성함으로써 유럽연합의 디지털 단일 시장(Digital Single Market) 환경을 조성하는 것을 목적으로 하고 있다[2]. 오랜 시간의 준비 기간을 거쳐 2016년 5월 제정되었으며, 2년간의 유예기간을 거쳐 2018년 5월 25일에 본격 시행되었다.

GDPR은 EU 내의 법적 구속력뿐만 아니라 전 세계 기업 규제 환경의 큰 변화를 초래하는 시발점으로 주목받고 있다. 이는 개인정보 범위의 확대, 정보 주체의 권리 및 컨트롤러/프로세서의 의무 강화를 비롯하여 기업의 책임성을 강화하는 조치들이 포함되었기 때문이다. 특히 개인정보의 국외이전과 관련하여 '적정성 결정(Adequacy decision)'을 근거로 허용하고 있으며, 적정성 결정이 없는 경우 '적절한 안전 조치(Appropriate safeguards)'를 통한 이전을 규정하고 있다.

적절한 안전 조치의 첫 번째 항은 표준데이터 보호조항(제46조 제2항c, Standard Data Protection Clauses, SCC)로서 EU집행위에 의해 승인된 표준양식의 정보 이전 계약서로 계약을 체결한 경우를 말한다. 두 번째는 구속력 있는 기업규칙(제47조, Binding Corporate Rules, BCR)으로 다국적 기업 내부에 구속

Table 1. The basis for the transfer of EU personal information over the GDPR

Category	Case	Details
Adequacy decision	Adequacy Assessment (National Level)	The EU Commission determines that the level of protection of a particular country corresponds to the EU.
Appropriate safeguards	Standard Data Protection Clauses(SCC)	Contract with information transfer agreement of standard form approved by EU Commission
	Binding Corporate Rules (BCR)	Establishment of binding guidelines and approval of authorities that are binding on multinational corporations
	Code of Conduct	Establish a code of conduct binding on corporate associations and international organizations and approve the authorities
	Certification Mechanism	Obtained certification of the personal information authentication system approved by the authorities
Exceptions	Consent of Information Authority	The information subject expresses positive statements through statements, positive actions (explicit consent)

력을 갖는 보호 지침 마련 및 당국 승인을 득한 경우이다. 세 번째는 행동 강령(Code of Conduct)에 의한 것으로 기업의 협회나 국제기구 등을 구속하는 행동 강령 마련 및 당국의 승인을 얻은 경우이며, 네 번째는 인증제도(Certification Mechanism)로 당국의 승인을 받은 개인정보보호 인증체계의 인증을 획득하는 방법이다. 이 외에도 예외사항으로 인정하는 경우(제49조)가 있는데, 정보 주체가 명시적인 동의로써 진술 및 적극적 행동을 통해 긍정의 의사표시를 한 경우이다. 한국의 기업들은 현재 주로 표준데이터보호조항(SCC) 또는 본인의 명시적 동의를 이용해서 개인정보를 역외이전 시키고 있다.

2.2 EU 개인정보보호 적정성 평가

2.2.1 EU적정성 평가란?

'EU 적정성 평가'는 EU 외의 국가가 EU와 동등한 수준의 개인정보보호 규정을 가졌는지에 관한 평가이다. 적정성 평가를 통과한 국가에서는 EU 시민의 개인정보를 해당 국가로 자유롭게 이동 및 활용할 수 있다. 이는 개인정보가 해당 국가로 이전되었을 때에도 '적정한 보호 수준(Adequate level of protection)에서 정보 보호가 이루어질 것으로 간주하는 것이다. EU 집행위가 말하는 '적정한 보호 수준'을 판단하기 위한 기준은 개인정보를 둘러싼 환경을 종합적으로 고려하는데,[3] 개인정보의 성격, 개인정보의 처리 목적과 기간, 개인정보의 최초 이전국과 최종 도착국, 제 3국에서 시행되고 있는 법률 규정, 직무규정 등 보안 조치 등이 해당된다.

현재 적정성 평가를 통과한 국가는 12개 국가로 뉴질랜드, 우루과이, 이스라엘, 스위스, 캐나다, 아르헨티나, 안도라, 페로 제도, 저지(Jersey), 맨 섬(Isle of man), 건지 섬(Guernsey), 미국 등이다. EU 협의회는 어떤 국가와 적정성평가 절차를 진행할지에 대한 기준을 가지고 있는데, 가장 우선시 되는 것은 해당 제3국과 EU가 실질적으로 또는 잠재적으로 어느 정도 상업적인 관계를 맺고 있느냐 하는 것이다. 일본의 경우에도 EU-일 간 FTA 협정 체결과 적정성 평가를 동시에 진행함으로써 양국 간 공조체제를 강화하고자 하고 있다. 두 번째로는 EU로부터 개인정보가 이전되는 범위에 관한 판단으로, 문화적/지리적으로 양 국이 얼마나 밀접한 관계를 맺고 있는지가 고려 대상이 된다. 세 번째는 대상국이 속해있는 지역에서 개인정보보호와 관련하여 얼마나 선도적인 역할을 수행할 수 있는지 영향력에 관한 판단이며, 마지막으로 EU와 해당국 간의 전반적인 정치적 관계, 즉 국가적/국제적 수준에서 공동의 목표를 지향하고 있는가를 고려한다.

이와 같은 판단에 의거 EU 협의회는 2017년 1월 10일 발표된 연락문서[4]를 통해, 아시아 지역에서는 한국과 일본을 적정성 평가 우선 대상국으로 선정하였으며, 향후 인도 및 중남미 국가로도 대상국 지정을

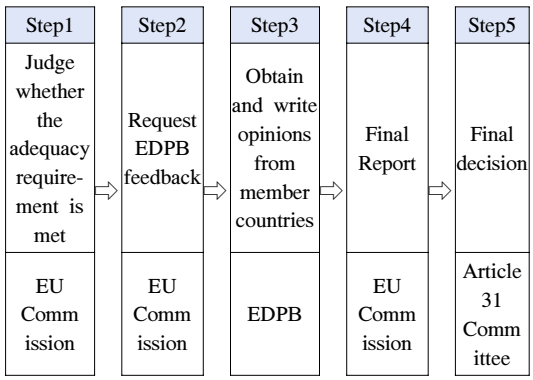

Fig. 1. EU Adequacy decision procedure

확장할 것을 밝힌 바 있다.

2.2.2 EU적정성 평가 절차

EU 적정성평가 절차는 크게 다섯 단계로 이루어진다. 신청국이 자체평가를 통해 적정성 평가를 의뢰 하게 되면 먼저 EU 집행위가 진행 과정에서 신청이 거부되지 않도록 평가 기준의 충족 여부를 판단하게 된다. 이 과정에서 신청국은 EU의 기준에 맞도록 자국 내 관련법을 제정 및 시행할 수 있다. 이와 같은 절차를 통해 EU 집행위가 신청국이 적정성 요건을 충족한다고 판단하면, 29조 작업반 내에서 EU 개인정보보호 감독기구인 EDPB(European Data Protection Supervisor)를 통해 각 회원국 별 검토 및 의견을 수렴하게 된다. 이 과정에서 다양한 사례별로 자료수집 및 면담, 정보 이전 실태조사 등이 이루어지며, 이를 바탕으로 최종보고서가 작성되고 31조 위원회에서 다수결에 따라 최종 결정이 이루어지게 된다.

Ⅲ. 아시아 대상국 추진 현황

3.1 일본

3.1.1 추진경과

일본은 2014년부터 정부 차원에서 EU 집행위원회와의 접촉을 시도하며 적정성 평가를 준비하기 시작했다. 특히, 2016년 4월 이후 일본과 EU 양국은 적정성 결정을 위한 상호 합의를 진행하였으며, 2017년 1월에 적정성 우선 평가 대상국으로 아시아에서 일본과 한국이 지정되면서 2017년 3월 20일, 브뤼셀에서 EU 집행위원과 일본 대표부의 면담을 추진하는 등 매우 적극적으로 협상에 돌입하였다.

특히 일본은 EU에서 자국으로 이전되는 데이터에 대해 다양한 보호 장치(safeguard)를 통해 '법령을 개정하지 않는 형태의 해결책'을 추가로 제시하였다. 2018년 2월, 4월에 제시된 가이드라인 및 2018년 9월에 발표한 보조규정에는 GDPR에서 요구하는 구체적인 수준의 개인정보보호 규제를 포함한 것이다. 이를 근거로 2018년 9월 5일 EU 집행위는 일본이 GDPR에 부합하는 수준의 데이터 보호를 제공한다는 '적정성 결정'을 승인하기 위한 내부 행정절차에 착수했다고 발표했다.

이는 양국의 상호 데이터 역외이전에 대한 합의가 이루어졌으며, 이후 유럽 개인정보보호 이사회의 의견 검토 및 EU 회원국 대표들의 허가를 거쳐 최종 승인되는 절차만 남겨두고 있다는 것으로 2018년 연내에 적정성 인정 프로세스 완료가 가능할 수준의 진전이 있었음을 의미한다.

3.1.2 주요 이슈

일본은 GDPR 제정에 대비하여 개인정보보호법 개정을 포함한 법제도 정비와 EU와의 협의를 적극적으로 진행해 왔다. 대표적으로 2015년 9월에 개정된 개인정보보호법은 GDPR에서 요구하는 수준의 규제 조치를 상당 부분 반영하고 있으며, 이를 근거로 개인정보보호와 관련한 여러 선도적인 조치를 취해왔다. 대표적으로 법 개정을 통해 독립된 제3자 데이터 보호기관을 설립하였고(2016년 1월), 5000인 이하의 개인정보 보유 사업자에게도 개인정보보호법을 적용하는 등 소규모 사업자에게로 규제 범위를 확대하였다. 또한, 데이터 이전에 대한 사업자의 권한 제한 등이 핵심적으로 포함되었다[5].

법률 개정 외에도 일본 정부는 국가적 차원에서 개인정보보호의 수준을 향상하기 위한 정책적 노력을 기울였다. 특히 EU에서는 적정성 평가 신청 후라도 진행 과정에서 '법령을 개정하지 않는 형태의 해결책'을 제시할 수 있도록 하고 있는데, 이에 대응하여 일본 정부는 개인정보보호 '가이드라인' 및 '추가조치'를 발표하였다. 추가조치는 크게 다섯 가지 항목에 대해서 진행되었는데, 민감정보처리, 보유 개인 데이터, 이용목적 특정, 제 3자에게 정보제공 제한, 익명 가공정보 등이다.

민감정보의 경우, GDPR에서 명시한 성적 취향, 노동조합 등에 대한 정보 등도 필요배려개인정보에 포함함으로써 민감정보의 범위를 확대했다. 또한, 보유개인 데이터는 개인정보 취급사업자가 공개, 수정, 추가, 삭제, 이전 등의 권한을 가지고 있는 개인 데이터인데, 기존에는 6개월 이내에 삭제 예정인 경우 보유개인 데이터로 취급하지 않았으나 추가조치에서 기간 한정 예외조항을 삭제시켰다. 이용목적 특정에 관한 항목은 EU에서 이전된 데이터에 한해서는 데이터 취득 시 확인 및 기록한 이용목적 내로 개인 데이터의 활용을 제한하는 조치이다. 개인 데이터의 재이전에 관한 규정도 강화하였는데, 일본에서 EU외 3국으로 데이터를 재이전 하는 경우 본인이 동의하는데 필요한 데이터를 제공해야 하며 GDPR과 동일한 수준의 보호조치를 시행하도록 하였다. 마지막으로 익명가공정보 처리의 경우, 가공방법에 대한 정보를 삭제하고 재확인이 불가능 하도록 조치하는 등 가공방법에 대한 정보가 남아있을 경우 이를 익명화되었다고 인정하지 않는 수준으로 익명성에 대한 규정을 강화하였다.

Table 2. Japanese Government Guidelines for GDPR Adequacy Assessment

Clause	Corrections	Details
Sensitive information	Extending the range of sensitive information	Special Categories of Personal Information in GDPR (information on the union, sexual orientation, etc) will be handling like sensitive personal information.
Retained personal data	Expansion of the scope of personal data held (deletion of time-limited exception clause)	For the personal data transferred from the EU, treat as personal data regardless of the period of retention.
Purpose of use	When the data is acquired, the purpose of use can be confirmed and recorded and should be used within the confirmed range.	For personal data transferred from the EU, limit the use of data within the scope of confirmed purpose when it was acquired.
Limit information provision to offshore third party	Enhance protection when transferring personal data from Japan to countries outside the EU.	If personal information transferred from the European Union is relocated according to the user's consent, information about the destination status of the data should be provided, and implement the same level of protection as the Personal Information Protection Act.
Anonymous processing information	Eliminate information about anonymous processing of personal data	Personal data transferred from the EU should be processed anonymously under the Personal Information Protection Act. Information on the machining method should be deleted and can not be reconfirm.

EU규제와의 상이함을 보완하기 위해 일본이 도입한 해당 규정 및 장치들은 향후 한국 등 적정성 평가를 진행하는 여러 국가가 참고로 활용할 수 있을 것이다.

3.2 한국

3.2.1 추진경과

한국은 2015년 10월부터 정부차원에서 EU 집행위원회와 접촉을 시작했으며, 범정부 차원에서 적정성 평가를 통과하기 위한 협의에 돌입하였다. 그러나 2016년 10월, 한국의 개인정보 보호기관(개인정보보호위원회)의 적격성이 미비하다는 이유로 EU 집행위로부터 평가 불가 통보를 받아 전체적정성 추진이 중단되었다.

이후 정부는 단계적 추진으로 방향을 전환하기로 하고, 2017년 3월에 우선 1단계로 정보통신망법 중심의 부분 적정성 평가를 추진, 전체적정성 평가는 2단계로 추진하기로 결정하였다[6]. 이때부터는 행정안전부가 책임을 맡아 방송통신위원회(이하 방통위)를 중심으로 '부분 적정성 평가'를 우선적으로 추진하기 시작한 것이다. 이는 범정부 차원에서 전체 적정성평가를 추진했던 초기 시도와는 차이를 보이는 점인데, 방통위는 포괄적인 개인정보보호법이 아닌 인터넷 상 개인정보를 다루는 정보통신망법을 담당하기 때문에 정보통신망법에 한해서만 부분 적정성 평가를 추진하게 된 것이다.

이와 같은 결정에 따라 방통위는 2017년 11월 20일 EU 사법총국에서 EU-한국 간 개인정보보호와 정보유통에 대한 '상호협력강화'를 골자로 하는 공동성명을 발표[7]하며 EU '부분 적정성 평가'를 추진한다는 점을 공식화 하였다.

그러나 개인정보보호위원회는 이미 EU 집행위로부터 지적받은 바대로 개인정보보호위원회의 독립이 우선되어야 한다는 점을 들어 부분 적정성 결정 추진을 중단할 것을 골자로 하는 '권고' 결정문을 2017년 11월 의결하며 방통위 결정에 반발하는 등 갈등 양상을 보였으나[8] 부분 적정성 평가는 방통위를 중심으로 지속적으로 추진되었다.

이후 약 1년여간 추진된 부분 적정성 평가에 대해 2018년 11월, EU가 다시 한번 부적합 판정을 통보함에 따라 적정성 평가는 새로운 국면을 맞이하게 되었다. EU는 한국의 개인정보보호기구가 독립되어 있지 않고 한국 정부가 요청한 평가 범위가 협소하다는 점을 들어 '부분 적정성 평가'가 아닌 '전체 적정성 평가'로의 전환을 요청하였다[9]. 이에 정부는 현재 각 부처로부터 입장을 취합한 뒤 적정성 평가 추진 방향을 논의 중에 있다.

3.2.2 주요이슈

우리나라도 개인정보보호법 및 관련 4개 법(정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보보호법, 위치정보의 보호 및 이용 등에 관한 법률, 전

기통신사업법)과 관련하여 보호 수준을 높이는 개정 노력을 꾸준히 진행해 왔다. 2015년 7월에는 개인정보보호위원회의 기능을 강화하고 징벌적 손해배상 제도를 신설하였으며, 2016년에는 주민 번호 암호화 적용 및 개인정보 수집 출처와 처리 목적고지 의무화, 민감정보, 고유식별정보 보호 강화를 골자로 하는 법령 개정이 이루어졌다. 2017년에는 법령 근거 없는 주민 번호 파기 의무화 등 주민 번호 처리 제한이 강화(공포 '16.3.29, 시행 '17.3.30)되었으며, 정보 주체 보호 강화를 위한 항목도 추가되었다.

특히 2018년에 의결 및 발의된 개정안들은 GDPR에서 요구하는 개인정보보호 방향과 수준에 근접하는 진전을 보이고 있다. 2018년 9월 11일 의결된 정보통신망법 개정안에서는 '개인정보 국외 재이전 시 보호 강화' 및 '해외 사업자의 국내 대리인 지정제도 도입'을 골자로 하고 있다[10]. 정보 재이전과 관련해서는 정보통신서비스 제공자가 국외 이전한 이용자의 개인정보를 제3국으로 재이전 하는 경우, 국외이전과 동일하게 원칙적으로 이용자의 동의를 받고, 기술적·관리적 보호조치를 취하도록 한 것이다. 이는 일본의 가이드라인에서 제시된 '제3자에게 정보제공 제한'과 유사한 항목으로 GDPR의 보호 수준을 충족하고 있다. 대리인 제도의 경우에도 국내에 주소 또는 영업소가 없는 정보통신서비스제공자 중에서 매출액 또는 이용자 수 등 일정 기준을 충족하는 사업자는 국내에 주소가 있는 대리인('국내 대리인')을 지정하도록 의무화하였다. 이는 해외 사업자의 개인정보 보호 의무를 강화하는 것이다.

또한 2018년 11월 15일 발의된 개인정보보호 관련 법률 개정안에서는 가명 정보 도입, 거버넌스 체계 효율화, 개인정보처리자의 책임 강화 및 개인정보 판단 기준 명확화 등의 내용이 포함되었다[11]. 특히 거버넌스 체계 효율화의 경우, 개인정보보호 감독기구를 개인정보보호위원회로 일원화하는 내용을 담고 있어 개인정보보호위의 기능 및 역할이 강화됨에 따라 EU 집행위에서 강조하는 '감독기관'에 대한 조건을 충족하기위한 초석이 될 수 있다. 그 외 개인정보처리자의 책임 강화는 일본의 가이드라인에서 제시하는 '익명가공정보' 처리와 유사하게 가명 정보를 복원하기 위한 추가정보와 관련한 내용을 담고 있다.

그러나 오히려 GDPR의 방침과 어긋나는 정책이 시행되어 우려되는 측면도 있다. 가명 정보 개념 도입에 관한 개정안은 개인정보를 개인 동의 없이 활용할 수 없다는 원칙의 예외로 가명 정보에 한해 산업적 연구목적의 활용을 허용하고 있다. 이는 개인정보의 순수 연구목적만 허용하는 GDPR 정책과 달리 개인정보가 산업연구 명목으로 기업 간 이전되거나 가명 정보 간 결합을 통해 개개인을 프로파일링 할 위험이 존재하는 등 우려를 낳고 있다.

Ⅳ. 정책적 시사점

본 연구의 목표는 우리나라가 EU 개인정보보호 적정성평가를 통과하기 위한 정책적 시사점을 도출하는 것이다. 이를 위해 앞장들에서는 적정성 평가 내용 및 평가절차를 검토하고, 아시아 우선 선정국가인 일본과 한국의 추진 현황을 파악하며 적정성 평가 진행에 있어 법률적·정책적 주요이슈들을 분석하였다.

이러한 분석을 바탕으로 본 논문에서는 향후 추진 방향을 4가지로 제시하고자 한다. 첫 번째는 개인정보 활용에 대한 가이드라인 및 추가 규정 제시이다. 우리나라는 최근 개정한 개인정보보호 관련 규정들에서 GDPR의 요구 수준에 근접하는 형태의 세부 보호 규정을 제시하였으나, 개인정보의 산업적 연구목적 활용 허용 및 통계 목적의 상업적 활용이 가능하게 하는 등 여전히 GDPR에서 요구하는 보호 수준과 상충하는 부분들이 존재한다. 이 같은 경우, 일본 정부와 같이 가이드라인 및 보조규정 등을 통해 법령을 개정하지 않는 형태의 해결책을 마련하는 방안이 유용할 수 있다. 이를 위해서는 정보의 속성과 산업별 특성을 반영해 신뢰할 수 있는 제3의 기관(Trusted Third Party)이나 전문가를 활용하여 다양한 제도적 장치를 마련해야 할 것이다.

두 번째로, 적정성 평가 범위의 확실한 재검토이다. 한국 정부는 전체 적정성 평가에서 부적합 판정을 받은 이후 기업 활동 지원과 개인정보 이슈가 오프라인에서 온라인으로 넘어간 상황에서 온라인 문제를 규정한 정보통신망법 적용을 우선 추진할 필요가 있다는 이유를 들어 부분 적정성 평가를 추진해 왔다. 그러나 부분 적정성 평가를 할 경우 적용 기업이 많지 않아 효과가 크지 않고, 국내에서는 개인정보보호법이 우선 적용되는 일반법인 데 반해 정보통신망법은 특별법이라 정보통신망법만 우선 적용하는 평가 자체가 부적절하다는 비판이 있어왔다.[12,13] 특히, 우리나라 EU 진출기업 규모는 총 697개[14]이며, 2017년 10월 개인정보보호위원회에서 EU 진출 모기업 380개를 대상으로 실태조사[15] 한 결과 94개 기업 중에서 인터넷 및 모바일을 이용하여 개인정보를 50% 이상 수집하는 기업은 8개, 5개 기업은 표준계약서 등 적정성결정 이외의 방법으로 이미 이전 중으로 부분 적정성 결정

으로 인한 실질적 혜택을 받는 기업은 극소수에 불과한 것으로 나타났다.

또한, 현재까지 적정성 평가를 통과한 국가(12개국) 중에서 부분 적정성 평가를 체결한 국가는 캐나다와 미국으로 2개국에 불과하다. 캐나다의 경우 상업 분야 전체를 대상으로 한 부분 적정성 결정으로 모든 진출 기업을 대상으로 해서 해당 범위가 매우 넓은 것으로 볼 수 있다.[16] 또한, 미국의 경우 프라이버시 쉴드(Privacy Shield)협약[1]을 통한 부분 적정성 결정이 진행되었는데, 프라이버시 쉴드가 미국으로 전송된 EU 시민들의 개인정보에 대한 안전장치와 기업들의 정보보호를 위한 의무사항을 GDPR과 동등한 수준으로 정하고 있고, 이 규약에 자발적으로 등록한 기업에 한해 EU 자국민 정보의 국외이전이 가능한 만큼 이 또한 적용 분야가 매우 넓다고 볼 수 있다.[17]

한국 정부는 EU 협의회의 부분 적정성 평가 부적합 결정에 따라 현재 향후 추진 방향을 논의하고 있다. 그러나 국내 개인정보보호법제의 신속한 개선 및 실효성 측면에서 전체적정성 평가가 추진되어야 할 것이다.

세 번째는 범정부 차원의 추진체계 구성 및 추진과정의 투명성 확보이다. 부분 적정성 평가가 아닌 전체 적정성 평가로 재전환 될 경우, 이전과 같은 단일 부처(행정안전부) 및 위원회(방송통신위원회) 수준이 아닌 범부처 수준의 협력체계 및 위원회 구성을 통한 추진이 필요하다. 이는 최근 산업 분야 간 융합의 결과로 각 부처 간 담당 산업 분야가 모호한 분야에서 산업별 특성 등을 고려하고자 할 때 더욱 필수적이라고 볼 수 있다. 예를 들어, 온라인 거래상 은행 이슈의 경우 통신법의 적용을 받지만 동시에 일부 금융위원회 소관 신용보호법으로 옮겨져 해당 부처 간 협력이 요구되는 것이다.

또한, 범정부 차원의 추진체계에서는 기존의 유사·중복된 법률 규정 및 감독기구의 체계화가 필수적일 것이다. 그간 개인정보보호 관련 법령은 「개인정보 보호법」, 「정보통신망 이용 촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」 등 으로, 감독기구는 행정안전부, 방송통신위원회, 금융위원회, 개인정보보호위원회 등으로 각각 분산되어 있어 체계적 정비 필요성이 각 계로부터 제기되어 왔다. 따라서 적정성 평가를 계기로 감독기구를 일원화하고, 관련 규정을 재정비할 필요가 있다.

1) 프라이버시 쉴드(Privacy Shield): 미국이 EU의 개인정보보호 기준에 부합하기 위해 국내법을 정비하는 대신 분야별 규제와 자율규제에 위임해 온 기존 제도를 유지하면서 GDPR의 요구사항에 부합되도록 협의한 규약(2016년 7월 12일 발효)

Table 3. Proposed suggestions to pass EU Adequacy decision of Korea

No	Suggestions
1	Establishment of supplementary regulations and guidelines related to the scope of information utilization
2	Extending the scope of adequacy assessment: from “part” to “whole”
3	Composition of the governance structure at the pan-government level
4	Independent guarantees of privacy provisions

마지막으로 개인정보보호위원회의 실질적 독립성 확보가 필수적이다. 개인정보 관련 감독기구의 독립성은 한국 정부가 두 번의 부적격 판정을 받으면서 공통적으로 지적된 사항이다. 한국 정부는 이에 대응하기 위해 개인정보보호위원회가 개인정보보호 정책과 감독을 전담하는 행정기구로의 독립을 추진하고 있다(2018년 10월)[18]. 그동안 중앙행정기관이 아닌 위원회 성격으로 운영되어 온 개인정보보호위원회가 중앙행정기관 수준으로 승격하는 것이다. 이렇게 될 경우 행정안전부, 방송통신위원회 내 개인정보보호 관련 업무가 위원회로 이관되고, 개인정보보호 정책과 협력, 정보 기반 보호와 정보 자원 정책을 담당하는 정보기반보호정책관 또한 위원회 산하로 이관한다.

이와 같은 움직임은 매우 환영할 만한 조치나, ‘독립성’의 의미를 다시 한번 살펴볼 필요가 있다. 현재 정부가 추진하고 있는 독립된 개인정보위원회는 1) 대부분 업무를 국무총리가 감독하고 2) 신용정보와 관련한 금융위원회의 권한이 유지되며 3) 위치 정보와 관련한 방통위의 권한이 유지되고 4) 시민단체·소비자단체의 위원 추천권을 없애고 공무원을 위원으로 선임하게 하고 5) 모든 위원을 대통령이 임명하도록 하고 있다[19]. 이는 GDPR에서 말하는 “감독기관의 완전한 독립”, 즉 정부의 규제 완화 조치 등을 견제할 수 있는 실질적 권한을 가진 기구로서 개인정보보호위원회가 기능하기 어려운 구조라고 볼 수 있다.

EU 개인정보보호 적정성평가는 국내 개인정보 보호 수준을 국제적 수준으로 높이고, 우리 기업의 EU 진출을 가속화 할 새로운 기회이다. 즉, 일차적으로는 최근 IT 서비스를 제공하기 위해 필수로 여겨지고 있는 고객 관련 정보, 즉 소비패턴, 마케팅 포인트 분석 등 데이터 분석을 통한 서비스를 EU 시민을 대상으로 제공하고자 할 때 개별 기업이 EU 내 개별국가(28개)별 법률 적용 및 검토에 소요되는 비용과 시간 낭비

없이 비즈니스가 가능해진다는 것을 의미한다. 이는 적정성 평가 통과가 국내 우수 IT업체 및 기술들을 기반으로 한 서비스가 독립적으로, 혹은 유럽 업체들과의 사업제휴를 통해 EU라는 큰 시장을 확보하는 가장 기본적인 초석을 다지는 일이 된다는 것을 보여준다. 예로, 지난 2019년 2월 스페인 바르셀로나에서 개최된 세계적으로 가장 큰 IT업계 행사 중 하나인 모바일 월드콩그레스(MWC) 2019에 참여한 국내기업들이 유럽 업체들과 GDPR로 인한 '데이터 거래 장벽'으로 인해 수많은 사업제휴 기회를 확보하기 어려웠다는 점[20]을 가볍게 봐서는 안 될 것이다.

이차적으로는 적정성 평가를 통해 궁극적으로 국내의 개인정보보호 수준을 국제적 수준으로 향상함으로써 향후 데이터 산업의 혁신과 발전을 이끄는 것을 목적으로 볼 수 있다. 최근 가장 쟁점이 되고 있는 4차 산업혁명은 데이터 경제(Data Economy)를 기반으로 작동한다고 해도 과언이 아닐 것이다. 데이터가 세계경제의 신 자본(New Capatal)으로 작동하는 미래사회에는 데이터의 확보 및 활용이 과거 산업혁명 시대에 원유를 확보하는 것만큼이나 중요한 일이 될 것이며, 이러한 사회에서 데이터 활용을 위한 사회적 안전망이 얼마나 잘 구축되어있는가는 향후 미래사회를 대비하는 가장 중요한 일 중 하나로 인식되어야 할 것이다.

우리나라는 이미 적정성 평가에 두 번의 실패의 경험이 있다. 이와 같은 실패를 반면교사로 삼아 중장기적 시각으로 관련 법규 및 제도를 개정해 나가고 EU 협의회 및 관련 기업들과 적극적인 협상을 이어나간다면 아시아에서 두 번째로 적정성 평가를 통과한 국가로서 향후 글로벌 시장으로의 진출이 더욱 기대되는 결과를 맞이할 수 있을 것이다.

References

[1] I. H. Kim, "A study on the international standards and contents of personal information transfer," *The Constitution of the United States*, vol. 24, no. 1, Apr. 2013.

[2] European Commission, *Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers*(2017.01.10), Retrieved 2019.2.10. http://europa.eu/rapid/press-release_MEMO-17-15_en.htm

[3] M. Park, et al., "The main contents and implications of EU privacy protection evaluation," *Korea IT Technology Promotion Center Weekly Technol. Trend*, Jun. 27, 2017.

[4] EU Commission, *Exchange and protection of personal information in a globalized world*(Exchanging and Protecting Personal Data in a Globalised World)(2017.10.01), Retrieved 2019.02.01. https://ec.europa.eu/newsroom/document.cfm?doc_id=41157

[5] E. Y. Han, "Content and evaluation of the amendment of the personal information protection law of Japan," *Inf. and Commun. Broadcasting Policy*, vol. 27, no. 17, pp. 41-51, 2017.

[6] J. K. Keum, *Personal information protection Commission vs Korea Communications Commission, Personal information diplomacy conflict* (2017.12.05), Retrieved 2019.2.10. http://www.mediatoday.co.kr/?mod=news&act=articleView&idxno=140122#csidxe25df5f7d27c282a83b434933aa3542

[7] Korea Communications Commission, *Joint Statement on Cooperation on EU Personal Information Protection* (2017.11.21.), Retrieved 2019.2.10. https://www.gov.kr/portal/ntnadmNews/1252620.

[8] J. K. Keum, *Adequate Decision KCC presses, personal information evaluation, refused in EU*(2018.11.02) Retrieved 2019.2.10. http://www.mediatoday.co.kr/?mod=news&act=articleView&idxno=145317#csidx8eebac59bc1f23e9eaa59a3f17fec1e

[9] Same as No. 6

[10] Korea Communications Commission, *Introduced a system for strengthening the protection of personal information and re-transferring it overseas*(2018.09.11.), Retrieved 2019.02.10. http://www.korea.kr/policy/pressReleaseView.do?newsId=156293814

[11] Ministry of Public Administration and Security, *Data Regulatory Innovation. The blueprint came out.*(18.11.22), Press Releases.

[12] Privacy Commission, *Regarding the improvement of the EU Partial Suitability Evaluation Conversion Promotion*(2017.11.13.),

No. 2017-25-198.
[13] 7 civic groups, *Civil society opinion on the government's evaluation of the level of privacy protection of the European Union* (EU)(2018.06.21.), Retrieved 2019.02.10, http://bit.ly/2BBm9OS
[14] KOTRA, *Korean corporate directory operating overseas*, Korea Trade-Investment Promotion Agency, 2016.12.28.
[15] PIPC, *2017 Privacy Survey*, Personal Information Protection Commission, 2017.
[16] Same as No.10
[17] Same as No.2
[18] J. J. Park, *Privacy Commission becomes independent organization, Relevant department agreement* (2018.10.21.), Retrieved 2019.02.10., http://www.etnews.com/20181019 000283
[19] J. K. Keum, *Personal information organization independence? The president did not keep his promise*(2018. 11. 21.), Retrieved 2019.02.10, http://www.mediatoday.co.kr/?mod=news&act=articleView&idxno=145601#csidx162dd4792c62f9682c17738726d1008
[20] C. H. Song, Ministry of Industry "*Ministry of Public Administration and Security has responsibility of Information Security "Ministry of Public Administration and Security" Do not know about corporate issues" Responsibility Ping Pong.* (2019.03.19.), Retrieved 2019.03.21.,http://news.donga.com/3/all/20190319/94621525/1

박 효 주 (Hyo-ju Park)

2016년 2월 : KAIST 기술경영학 석사
2012년 8월~2014년 2월 : KAIST IT융합연구소 연구원
2016년 3월~2018년 8월 : 부산과학기술기획평가원 연구원
2018년 9월~현재 : 인제대 컴퓨터공학부 연구원
<관심분야> 과학기술정책, 개인정보보호, GDPR
[ORCID:0000-0002-7756-0263]

양 진 홍 (Jin-hong Yang)

2017년 2월 : KAIST 정보통신공학 박사
2017년 2월~2018년 1월 : HECAS 최고기술책임(CTO)
2018년 3월~현재: 인제대학교 헬스케어IT 학과 조교수
<관심분야> CPS, IoT 시스템, 프라이버시
[ORCID:0000-0002-5871-8387]