EU 적정성 결정이 GDPR 대상기업에 미치는 영향에 관한 탐색적 연구

[1] 김영수, [2*] 장항배

An Exploratory Study on the impact of EU Adequacy Decision on GDPR compliant companies

[1]YoungSoo Kim, [2*]Hangbae Chang

요 약

유럽연합은 자국민의 개인정보보호를 위해 강력한 규제 법령으로 GDPR을 2018년 5월 25일 시행하였다. 글로벌 경제 시대에서 유럽시장 진출 기업에서는 GDPR 대응은 꼭 필요한 선결 과제이다. 본 논문에서는 유럽 연합내 거주민의 개인정보 역외 이전을 위한 적절한 수준의 보호조치 대응을 위해 기업에서 준비해야 할 단계별 추진과제를 살펴보았다. 제3국에서의 GDPR 대응은 개별 기업 또는 정부차원의 대응을 할수 있으며, 정부차원의 적정성 결정시 기업의 혜택과 기대효과에 대해서 탐색해 보았다. 적정성 결정 국가의 기업에서는 EU 진출시에 프로세스 간소화, 비용 절감 등의 혜택과 유출사고 대응시 정부차원의 독립된 감독기구 지원으로 인한 부담감 해소 등에 따른 시사점이 있다. 그러나, 적정성 결정 이후에도 기업은 GDPR 원칙, 의무규제 준수를 통한 개인정보보호체계 확보 활동은 지속적으로 필요하며, GDPR 대응 과제에 대한 중요도 변화에 대해서도 유럽 국가와의 계약서 체결을 제외한 대부분 준수되어야 할 과제로 유지가 필요하며, GDPRR 대상 기업들의 차별화된 관리 방안 구축도 기대한다.

Abstract

The EU enacted a law strongly regulating the GDPR to protect the privacy of its citizens on 25 May 2018. Compliance with GDPR is an essential prerequisite for companies to enter the European market in the global economic era. In this paper, Step-by-step measures have been defined to conclude DPA agreements for the appropriate level of protection against EU personal data transfer. To explore the benefits and expected effects of determining appropriateness at the government level. As a result, enterprises benefit from simplifying processes, reducing time, and reducing costs when entering the EU. Government-level support in response to personal data breach and communication with the EU Commission will have a positive impact, However, even after the adequacy decision, the entity continues to need activities to secure personal data through compliance with GDPR principles and obligations. Major operations of companies that comply with GDPR are also maintained as important tasks that must be observed in most cases except for the Data Protection Agreement.

Keywords: *GDPR, Adequacy decision, Personal information Protection, SSC, DPA, Security Design*

[1] *중앙대학교 대학원 융합보안학과 석사과정 (ysookim19@cau.ac.kr)*
[2*] *교신저자 중앙대학교 산업보안학과 교수 (hbchang@cau.ac.kr)*

Received: July. 09, 2021, Revised: Aug. 24, 2021, Accepted: Sept. 28, 2021

I. 서론

4 차산업혁명 시대는 초연결 사회로 데이터 유통에 경계가 없이 활용 되어지며 ICT 기술의 발달에 따른 지능정보화 사회에서 개인정보는 핵심재료로 활용되어 지고 있다. 특히 ICT 융합기술을 활용한 클라우드 플랫폼 서비스인 아마존 웹서비스(AWS), 마이크로소프트 애저(Azure)등과 같은 글로벌 사업자가 제공하는 서비스만 보아도 국경 간 개인정보의 이동은 불가피한 현실이다.

이렇듯 개인정보가 국경의 경계가 없이 유통되면서 개인정보의 활용측면과 보호측면의 대응이 필요하게 되었고, 우리나라를 포함한 각 국가에서는 개인정보 데이터 취급에 대한 적절한 보호조치와 적법한 법을 근거로 보호되어야 함을 강조하였다. 유럽연합(European Union, 이하 EU 로 사용) 역시 미국에 기반을 둔 구글, 페이스북, 유튜브 등 글로벌 인터넷 플랫폼 서비스에서 자국민들의 개인정보를 보유하고 이동되고 있음에 강력한 개인정보보호 규제가 필요했으며[8], 기존의「개인정보보호지침(Directive95/46/EC)」은 새로운 기술의 도입에 따른 개인정보를 보호하기 어렵다는 평가와 EU 회원국별 상이한 제도와 법적 환경으로 자유로운 정보 이동을 제한하였다.

이는 EU 에서 목표로 하는 단일 시장의 발전을 저해하는 요인으로 작용하였다. 이에 EU 는 2018 년 5 월 25 일 GDPR 을 발효 시행하면서 EU 회원국에 직접적으로 적용되는 강력한 법적 구속력을 가질 수 있게 했다.

국내 기업들도 전통적인 제조업뿐 아니라 최첨단 ICT 기술이 적용된 다양한 서비스로 EU 시장 진출을 하였고, 개인정보와 직간접으로 연계된 서비스가 일반화된 상황이다. 국내 기업뿐만이 아닌 세계 각국과 협력하는 기업, 직접 해외진출 한 기업들도 개인정보를 이전받아 처리하는 경우가 증가하고 있다[13]. 또한 EU 도 비즈니스 친화적인 환경을 제공하면서 다양한 스타트업 유치에 적극적이다.

이와같이, EU 시장 진출은 GDPR 규제 준수와 위반시 높은 과징금에 대한 부담을 무시할 수 없으며, EU 시장에서의 경쟁은 포기할 수 없는 상황이다. GDPR 의 개정 중 가장 큰 변화는 영역의 확대 이다. EU 회원국 뿐만 아니라, EU 거주민들 대상으로 영업을 하는 모든 글로벌 기업들은 GDPR 대상이며 이를 위한 대응 준비가 필요하다[13].

EU 역외로 EU 거주민의 개인정보를 제 3 국으로 유통 및 활용을 위해서는 적정한 수준의 개인정보보호 체계를 갖추어야 한다(제 44 조~제 45 조). 이는 EU 진출기업, 진출 예정 기업이 GDPR 준수를 위한 첫 번째 관문이다.

국가차원에서 GDPR 과 동일한 수준의 개인정보보호 체계가 갖추어졌다고 인정되면 '적정성 결정' 이 적용된 국가가 된다. 우리나라는 현재 적정성 결정 국이 아니므로 개별 기업에서 GDPR 대응 준비를 해야 한다. 그러나, 기업의 규모와 GDPR 세부 규정의 이해도 등에 따라서 기업에서는 준비의 어려움이 발생하고 있으며 이로 인한 EU 진출이 지연 되고 있거나 포기가 일어나는 기업이 발생하고 있다.

따라서, 본 논문에서는 개별기업에서 GDPR 대응을 위한 방법 중 European Commission 에서 제시한 표준데이터보호조항을 참고하여 개별 기업이 GDPR 대응을 위한 단계별 과제를 도출하고, 현재 정부차원에서 준비하고 있는 적정성 평가 승인이 완료되면, 기업에 미치는 영향과 기업에서 GDPR 대응과제 변화 연구 및 고려해야 할 사항에 대해서 살펴보고자 한다.

II. 이론적 배경 및 선행연구

2.1 GDPR 도입 취지와 주요 변화

EU 회원국들은 상이했던 개인정보보호 수준으로 인해 경제활동에 장애가 될 수 있다는 인식이 널리 퍼졌었고, 회원국들의 일관된 개인정보보호의 필요성에 대한 해결책이 필요했다.

이에 GDPR 을 EU 내 일반법으로 모든 회원국에 동일하게 적용될 수 있도록 법 개정, 반영 및 수정을 하였다[2]. GDPR 은 종래의 지침 수준과 달리 법적 구속력을 가지며 모든 EU 회원국에 직접 적용된다(제 99 조). 이렇듯 GDPR 도입 취지는 첫째, 보다 강하고 일관성 있는 EU 차원의

개인정보보호체계를 확립함으로써 4 차산업혁명 시대의 디지털 경제의 개인정보 이동촉진 및 발전을 시키고, 둘째, 개인에게는 더 많은 자기정보에 대한 결정권을 부여하며, 셋째, 사업자에게는 법무적, 실무적 확실한 법적 규범과 담보를 확보하기 위함이다[11].

GDPR 은 강력한 법 규제로 시행되면서 다음과 같은 주요 변화를 주었다.

2.1.1 확대된 개인정보 범위 및 적용대상

GDPR 에서 개인정보는 '식별된 또는 식별될수 있는 자연인에 관한 모든 정보' 로 정의된다(제 4 조). 온라인 식별자, 위치정보, 추가 정보를 이용하여 개인을 식별할 수 있는 가명정보 등을 개인정보로 취급 하였다(제 9 조)[16]. 그러나 익명정보는 더 이상 개인을 식별할 수 없으므로 대상에서 제외 하였다.

GDPR 적용 대상의 주체는 컨트롤러와 프로세서 모두에게 적용이 되었다. 그러나 강력한 법제화가 되면서 프로세서의 법적의무가 주어졌다(제 79 조). 프로세서는 처리 활동의 기록(제 30 조), 적절한 보안기준 적용(제 32 조), 정기적인 개인정보 영향평가 수행(제 32 조), 개인정보 국외전송 기준 준수(제 5 장), 국가 감독기구 협조의무(제 31 조) 등의 법적 의무와 규제도 직접 적용되었다. 우리 기업은 프로세서 및 컨트롤러가 될 수 있으며 역할별 개인정보 보호를 위한 준수 사항에 대한 명확한 인식을 해야 한다.

2.1.2 개인정보 처리 원칙 기반 접근

'원칙기반 접근' 에 따라 개인정보 처리 원칙(제 5 조)을 확립하고 있으며, 개인정보 처리의 적법성 · 공정성 · 투명성 원칙, 수집 목적 제한의 원칙, 개인정보처리 최소화 원칙, 정확성 원칙, 보존기간 제한의 원칙, 무결성 · 기밀성의 원칙 등 6 가지 원칙이 강조 되었다. 컨트롤러는 상기 원칙을 준수할 책임을 지며 이를 입증 할 수 있어야 한다는 책임성의 원칙을 부담하였다(제 5 조).

2.1.3 정보 주체의 권리 강화

정보주체는 정보를 받을 권리(Right to be informed, 제 13 조,제 14 조), 정보주체의 열람권(Right of Access, 제 15 조), 정정권(Right of rectification,제 16 조), 삭제권(잊혀질권리) (Right of erasure,제 17 조), 처리 제한권(Right of restriction of processing,제 18 조), 개인정보 이전권(Right to data portability,제 20 조), 반대할 권리(Right to object, 제 21 조), 자동화된 결정(프로파일링 포함)(Right to related to automated decision making and profiling, 제 22 조)등 새롭게 추가 및 수정 되어 정보주체의 동의, 요구에 의한 처리와 권리를 강화 하였다.

2.2 기업의 책임성 강화와 위반시 영향

GDPR 의 가장 큰 특징은 지리적인 범위의 확장이다. EU 진출한 전세계 기업은 GDPR 규제 준수가 필수 사항이고, GDPR 은 전세계 개인정보보호법 정립의 기반이 될 것이다.

2.2.1 기업(개인정보 처리자)의 책임성 강화

개인정보 수집 기술의 발달로 기존 법제로는 수용할 수 없는 문제들이 발생되었고, 개인정보 처리자 책임성 강화를 도모하는 방안을 마련 하였다[13]. 책임성 강화 방안의 핵심은 개인정보 처리자의 의무를 강화하고, 확대하면서 새로운 규제방식인 자율규제를 도입하는 것이다.

GDPR 의 제 5 조 제 2 항 개인정보처리원칙에서 언급하고 있는 책임성 조항은 구체적인 조항을 통해 요구사항을 제시하였고, 이를 통해 개인정보 침해 등 위법의 위험을 최소화 하고 정보주체의 권리를 보장하고자 한다[13].

개인정보 처리 활동 기록 문서화 및 보유, 개인정보 보호적용 설계 및 기본설정(Data Protection by design and by default, 제 25 조), 개인정보 영향평가(Data Protection Impact assessment, 제 35 조), DPO(Data Protection Officer, 제 37~39 조) 임명과 역할, 승인된 행동규약과 인증제도(제 40~42 조) 등을 준수하여 개인정보를 처리 하였다는 것을 보장하고 이를 입증할 수 있게 조치를 이행 해야 한다.

2.2.2 위반시 기업의 영향

GDPR 은 대상기업에 각종 원칙에 대한 의무를 부과함과 동시에 위반시 거액의 과징금을 부과하고 있다. 일반위반의 경우, 전 세계연간 매출의 2% 또는 1 천만 유로 중 높은 금액을 부과하고(제 8 조,제 11 조), 개인정보 6 대원칙 위반, 처리 적법성 위반, 감독기구가 내린 명령 및 처리 불복 등과 같은 심각한 위반일 경우 최대 전세계 연 매출액의 4% 또는 2 천만 유로 중 높은 금액에 해당하는 징벌적인 벌금이 부과된다(제 5 조, 제 6 조, 제 58 조). 과징금은 개별 사건에서 부과 여부를 결정하고 과징금 액수를 결정할 때에는 개인정보의 성격, 범위, 목적을 고려하여 위반의 중대성, 손해의 정도 및 과실, 컨트롤러와 프로세서가 취한 조치사항(제 83 조) 등을 고려한다. 위와 같은 과징금은 기업의 존폐와 같은 심각한 영향도 끼칠 수 있다.

III. EU 개인정보 역외 이전과 GDPR 대상기업 대응과제 도출

EU 는 자국민의 개인정보보호를 위해 국외 이전을 엄격하게 제한하지만, 개인정보를 합법적으로 국외 이전 할 수 있는 다양한 방식을 제공하여 다른 나라의 개인정보 국외이전에 대한 제도와 충돌하지 않고 상호 호환이 가능하도록 배려하고 있다[8].

앞서 2 장에서 GDPR 주요 내용에 대한 이론적 배경과 선행연구를 살펴보았고, 3 장은 GDPR 대상기업의 개인정보 역외이전에 따른 원칙 준수를 위해서 대응해야 하는 과제를 준비 단계별로 도출하고자 한다.

4 장은 정부차원의 적정성 결정에 따른 기업에 미치는 영향에 대해서 살펴보고, GDPR 대상기업의 대응과제 변화에 대해서도 살펴보고자 한다.

3.1 GDPR 의 개인정보 역외이전 원칙

EU 시민의 개인정보를 국외로 전송하는 경우, 데이터를 전송 받는 제 3 국이 “적절한 수준의 개인정보 보호조치” 를 제공하고 있다는 것을 보장해야 한다. 국가차원의 적정성 결정을 받지 못한 경우에는 기업에서 EU 위원회로부터 ‘적절한 수준의 보호조치’ 에 대한 승인을 받아야 개인정보 역외 이전이 가능하며, 역외 이전 가능 조건은 표 1 과 같다[11].

Table 1. The Basis for the transfer of EU Personal data 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

현재 개별 기업에서 가장 쉽게 접근할수 있는 표준데이터보호조항(Standard Data Protection Clauses)은 EU 집행위원회에 의해 제시된 표준 계약서 양식을 사용하여 체결하는 방법으로 계약 절차가 간단하고 체결 즉시 보호조치가 인정된다는 점에서 장점이 있다[11]. 표준데이터보호조항을 기반으로 계약 체결을 위해서 기업은 제시된 구성 조항에 맞게 실제 기업 내 정보를 기술하고 GDPR 원칙을 준수하였다는 근거로 문서화 준비와 보호 강화 노력을 해야 한다. 표 2 는 유럽내 Controller 가 유럽외 Processor 간에 적용되는 계약서 조항이다.

Table2. standard contractual clauses for the transfer of personal data[4]

Clauses	Detail
Clause 1	Definition (Purpose and scope)
Clause 2	Details of the transfer
Clause 3	Third-party beneficiary clause
Clause 4	Obligations of the data exporter
Clause 5	Obligations of the data importer
Clause 6	Liability
Clause 7	Mediation and jurisdiction
Clause 8	Cooperation with supervisory authorities
Clause 9	Governing law
Clause 10	Variation of the contract
Clause 11	Sub-processing
Clause 12	Obligation after the termination of personal data-processing services
Appendix1	Categories of personal data transferred
Appendix2	Technical and organizational security measures

3.2 GDPR 대상기업 단계별 대응과제

GDPR 대상기업은 EU 와의 사업 활동을 새롭게 전개하거나 기존 활동을 적극적으로 유지하기 위해서 GDPR 을 기업마다 스스로 준비해야 한다. GDPR 준수는 기업내 조직에서 개인정보보호 인식제고부터 시작되며, 전체 조직이 준비 활동에 참여해야 한다.

다음은 앞서 제시한 표준데이터보호조항을 참고하여 GDPR 대응을 위한 단계별 과제를 정의한다.

3.2.1 준비 단계

GDPR 대상 시스템 선정 여부와 개인정보 현황을 파악하는 단계이다. EU 내에서 발생된 개인정보 보유 시스템 마다 존재하는 개인정보 유형, 범위, 사용 목적 등을 상세히 정의하고, 어떤 경로로 데이터가 유통되고 있는지 개인정보 흐름파악을 위해 Data Flow(인터페이스 현황, 백업 현황 등), Data mapping 정의서 등을 준비한다[17]. 이러한 개인정보 유형과 흐름의 파악은 정보주체의 권한 중 삭제권(잊혀질권리), 처리제한권, 이전권 등에 대한 요구시에 대응을 위함이기도 하다.

기업에서는 GDPR 대응을 위해 특정 조직에 한정되지 않고 법률 담당자, 시스템 담당자, 보안 담당, 개발자 등 전사의 모든 조직에서 GDPR 대응 수행을 위해 역할이 정의되고 대응 계획 및 일정을 결정해야 한다[17]. 표준데이터보호조항은 개인정보 역외이전 대상 시스템에서 활용하는 개인정보 유형 및 범위에 대해 정의하고[7], 처리 방식에 대한 근거 등을 매우 상세하게 정의하도록 요구 하고 있고, 명기된 실행 목적대로 준수 해야 한다.

준비 단계부터 개인정보보호 활동을 주도할 DPO 를 선임 해야 한다. DPO 선임기준 여부에 따라서 조직 내 또는 조직 외부에서 계약을 통해 확보 할 수 있으며, 개인정보처리 활동 역할에 전담 인력이 필요함을 요구한다[1].

3.2.2 GAP 분석 및 개선방안 수립 단계

현재 조직의 개인정보보호체계와 GDPR 에서 요구하는 규제의 차이를 분석하고 미흡한 부분을 중심으로 리스크 평가 및 대응 계획을 수립하는 단계이다[17]. 기업에서 대표적으로 진행하는 방법이 표준데이터보호조항을 기반한 계약서로 EU 개인정보 역외 이전 준비를 하고 있고, 계약서 작성을 위해서는 개인정보 수집 동의서 및 통지서, 개인정보 처리 방침 및 Controller 와 Processor 의 역할 정의, 손해배상 책임 범위 정의, 개인정보 처리를 위한 데이터 보안 설계 (Data Protection by Design and by Default), GDPR 관련 리스크를 최소화 하기 위한 프로세스 개선 등에 대한 준비가 필요하다. 특히 데이터보안 설계는 Technical and Organisational Security

Measures[15]의 요구 내용 기반으로 기술적 · 관리적 보호조치 및 보안통제 항목을 구체적으로 기술하고 현재 기업내의 보안관리체계와 보안 이행 지침 내용을 근거로 정의해야 한다.

즉, 기업내 개인정보 처리의 목적과 데이터 보호를 위한 원칙 준수에 대해서 입증할 수 있도록 내용을 문서화 해야 한다.

3.2.3 적용 단계

현황 분석과 개선 방안으로 수립된 미비한 사항을 개선하고, IT 시스템에 반영 및 적용을 위한 활동 이행 단계이다. 또한 새로 제정한 규정, 원칙을 조직 전체에 전파하고 운용이 이루어지도록 한다[9]. 적용된 기술 및 조직에서 수행한 구체적인 활동은 기업내 문서화된 IT 보안 정책에 준하여야 하며, 조치된 항목의 안전 수준은 기술적 진보와 발전에 대응되어야 하고, 안전 이하의 수준이 있으면 안된다.

자체 시스템별 영향 평가는 예를들어, 개인정보 DataFlow → 프로세스에 대한 현실성 확인 → 데이터 유출 사고에 대한 검증 → 온 · 오프라인 프로세스 점검등과 같이 구체적으로 기술하고 검증 수행하며, 상황 시나리오별 개인정보 위협에 대한 점검 및 개선이 수행 되어야 한다. 이러한 전반적인 활동에 누락이 없도록, '준비 → GAP 분석 및 개선방안 수립 → 적용 단계' 각 단계에서 도출된 과제에 대한 GDPR 법률 이행 점검표를 준비하여 누락이 없도록 체크 하여야 한다.

GDPR 대상기업의 단계별 대응 과제를 표 3 과 같이 정리한다.

Table 3. Key Task for GDPR compliant companies

Phase	Task	Detail
Preparation Phase	Organize GDPR TFT	Defining Role such as GDPR guides, legal experts for entering into contracts, security, application managers, IT security admin, system leadership, etc
	Identify the status of the EU Target system	• Checking the status of personal information processing and checking the target system
	Define Personal data Flow, Processing Type	• Identify the status of the personal information collection system ①Define the purpose of processing personal information ②Definition of type and scope of personal information ③Status of personal information processing tasks (collection, processing, relocation, disposal, etc) ④Define the status of the privacy flow chart (Interface status, Backup data archive, etc)
GAP Analysis and improvement Plan Design Phase	Designation of the DPO	• Designation based on DPO selection criteria
	Data Protection by Design	• Data Security design and improvement of deficiencies by comparing the privacy system within the current organization
	Preparing a contract (Data Processing Agreement)	• Personal information Collection Agreement and Notice • Personal information processing policy, etc • Controller & Processor Definitions (including roles) • Defining the scope of liability for damages The preparation step content is created in the contract
Action Phase	Appropriate security & Personal data protection measure	• Apply analysis and improvement plan • Apply Data Protection by Design • Application of improvements in measures to prevent and cope with infringement accidents
	Update IT System Improvements	• Apply existing system enhancements
	Data Protection Impact Assessment	Assessment and audit of the impact of the personal information system
Phase	Task	Detail
Action Phase	Set up and implement of Personal data breach procedures	①Notification immediately to supervisory ②Notify the subject of information if there is a possibility of significant risk
	Documentation & Training	• Policy for data breach/Incident management has been documented • Regular training for GDPR follow-up action has been scheduled/performed

IV. EU 적정성 결정과 국내기업 대응사례 분석 및 대응방안

4.1 EU 적정성 결정과 개인정보 역외이전 변화

‘적정성 결정(adequacy decision)’이란 유럽 위원회에서 EU 내 개인정보를 역외 제 3 국이나 국제 조직으로 이전하기 위해서는 적정한 보호수준을 보장하고 있다고 결정하는 제도이다. 이러한 적정성 결정을 받은 국가는 EU 역내에서 발생한 개인정보를 해당 국가로 이전하는데 추가적인 보호조치에 대한 승인 없이 EU 회원국들과 동일하게 역외로 개인정보를 이전할 수 있다. 적정성 결정을 위해서는 다음 요소를 고려해야 한다[12].

첫째, 정보주체의 권리 보장 및 권리 침해시 구제 수단 등이 완비된 개인정보 관련 법률 및 제도가 형성되어야 한다. 둘째, 독립성 · 집행력 있는 감독기구의 존재이다. 셋째, 적정성 결정의 지속적 유지를 감독기구의 주요 업무로 규정 해야 한다.

적정성 평가는 4 년마다 정기적인 심사를 한다(제 3 항). 적합한 보호수준을 보장하고 있지 않다고 판단하는 경우에는 소급효 없이 법령에 의해 적합성 결정을 폐지, 개정 또는 정지 시킬 수 있다[12]. 그림 1 은 적정성 결정을 위한 단계별 절차이다.

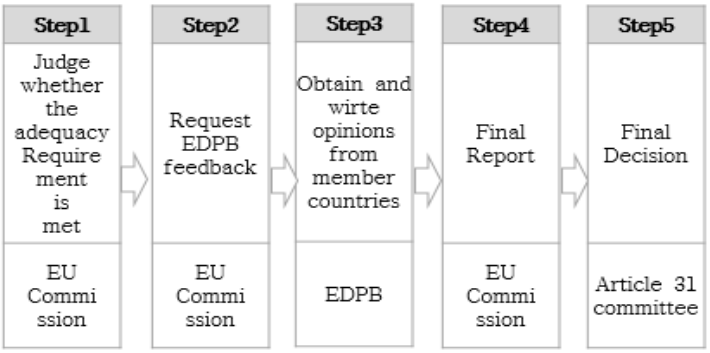

Figure 1. EU Adequacy Decision procedure

적정성 결정이 확인된 대상 국가의 기업은 EU 진출을 위해서 생성했던 표준데이터보호 조항이 포함된 DPA(Data Processing Agreement) 작성과 계약체결 단계가 생략되며, 이와 같은 혜택은 EU 진출 및 진출 예정인 기업에게 획기적으로 개선된 절차로 살펴볼 수 있다[6].

4.2 EU 적정성 결정과 국내기업 대응사례 분석 및 시사점

정부는 EU GDPR 대응 활동으로 클라우드, IoT, 빅데이터, 모바일 등 기술을 활용한 다양한 신사업을 주도하기 위한 핵심데이터 이용 활성화를 위해서 국내법인 「개인정보보호법」, 「정보통신망법」,「신용정보보호법」의 유관법제를 통합한 데이터 3 법을 2020 년 8 월 5 일 시행하였다. 위의 개정은 데이터 이용에 관한 규제 혁신과 개인정보보호 거버넌스 체계 정비를 해결하기 위함이다[9]. 이러한 정부의 노력과 함께 적정성 결정이 확정되면, 개별기업에서 EU 개인정보 역외이전을 위한 계약 등 사전 EU 진출을 위한 추가 규제 없이 EU 기업과 동등하게 영업활동을 가능하게 되어, EU 시장 진출 포기와 같은 상황은 해소 될 것이다.

적정성 결정으로 인해서 별도 개인정보보호 관련 현지 규제에 따른 부담과 불이익을 당하지 않는 등 기업에게 비용절감-편익증대 측면에 따른 아래와 같은 시사점을 갖을 수 있다[6].

4.2.1 적정성 결정에 따른 비용절감 측면

한국인터넷진흥원(2018)은 기업의 GDPR 대응 현황 조사 시 준비 비용은 평균 1.1 억, 적정성 결정 후 자체적으로 준비시는 40% 절감 될거라고 답변했다. 이와 같이 준비에 따른 ‘전문인력 및 물적비용’, ‘각국과의 심사비용’, ‘안전한 보호조치 수준 미달에 따른 추가 리스크 비용’, ‘채택이후 정기심사와 계약서 갱신, 연장, 재계약’ 등의 비용부담이 해소될 수 있다[6].

4.2.2 적정성 결정에 따른 편익증대 측면

표준데이터보호조항을 기반한 계약 체결을 위해서 기업에서는 ‘별도 준비가 필요 없고’, ‘EU 적시진출’, ‘EU 내 국내기업들의 개인정보보호 신뢰도 향상으로 개인정보 규제 부담과 불이익을 당하지 않게 되어 영업활동에 큰 도움’이 될 것이고, ‘GDPR 위반 이슈와 교섭시에 EU 위원회와 정부의 독립적 감독기구를 통한 소통과 협상’을 할 수 있다[13].

개별 기업에서 GDPR 준비 시 EU 거주민의 개인정보 이전을 위한 해당 국가와 계약서 준비, 체결까지의 과정이 생략된 편익에 대해서 사례를 통해 살펴 본다.

예컨대, 국내본사 중소기업(H)은 EU 역내지점(h)을 설치하여 무역거래를 하고 있는 경우에 h 가 관리하는 EU 거주민의 직원과 고객의 개인정보를 수집하여 국내본사 H 로 이전 시 적정성 결정으로 아무런 조치 없이 이전이 가능하다. 적합성 결정을 받지 않았다면, 표준데이터보호조항을 기반한 계약서 체결 준비에 따른 비용과 시간 등의 부담을 가질 수 있다[6]. GDPR 의 적정성 결정은 EU 내 거주민의 개인정보 이전을 위한 보호 차원만이 아닌, 국내기업의 글로벌 시장에서의 기업 경쟁력 향상과, 이미지 고취, 국가 차원의 개인정보보호 체계에 대한 위상 등 비용절감과 편익의 효과성 측면에 시사점을 주고 있다.

4.3 EU 적정성 결정에 따른 국내기업 대응과제 도출

기본적으로 적정성 결정을 받은 국가의 기업은 EU 내 개인정보 역외 이전이 별도 조치 없이 가능함을 앞서 설명하였다. 여기서 별도 조치가 필요 없다는 것은 기업내의 안전한 개인정보보호 조치 증빙인 표준데이터보호조항을 기반한 계약서 작성과 EU 진출국에서의 승인이다. 그러나, 기업에서 개인정보 보호와 처리에 대한 책임 및 의무 규정 준수는 변함이 없다[12].

앞선 사례를 통해 국내본사 H 사와 EU 역내 h 사는 개인정보 처리와 관련하여 컨트롤러와 프로세서로서 의무 준수를 해야 하는 것에는 변함이 없다.

EU 현지에서 적정성 결정이 인정된 국가로의 데이터 이전은 아무런 조치 없이 이전이 가능하지만 적정성 결정 국가가 아닌 제 3 국의 법인, 지점으로 이전시에는 적절한 보호조치 체결이 필요하다. 이와 같이 EU 내 개인정보 이전시 적정성 결정 국가 여부의 판단부터 컨트롤러, 프로세서의 의무 준수 또한 기업의 몫이다.

다음은 GDPR 대상기업의 대응 과제로 도출된 11 개 과제에 대해서 적정성 결정 전 · 후 기업의 대응과제에 대한 중요도 변화를 전문가 집단을 통해 알아보기 위해 설문 조사 연구를 하였다.

4.3.1 조사 내용

- 조사 목적: 적정성 결정 후 기업의 GDPR 대응과제 중요도(우선순위) 변화 예측을 위한 전문가 의견 수렴
- 조사 대상: IT&보안, 법률, 컨설턴트 관련 전문가 – 33 명
- 조사 내용: 기업에서 GDPR 준수를 위한 과제에 대해서 적정성 결정 전 · 후 중요도를 리커트 5 척도로 응답하도록 구성
- 조사 방법: 온라인을 통한 자기기입식

4.3.2 연구 결과

표 4 는 GDPR 대상 기업의 GDPR 대응을 위한 도출된 과제 11 개에 대해서 정부차원의 GDPR 대응인 적정성 결정 이후 기업의 대응 과제별 중요도 변화에 대한 설문조사 결과이다.

평균값(Average)의 전 · 후 비교 결과는 모든 과제에 대한 점수가 적정성 결정 이후 전체적으로 낮아졌다. 그중에서도 기업내 개인정보 현황과 관련된 ‘개인정보 범위, 흐름, 처리 유형 파악’, ‘개인정보 보유시스템 현황 파악’ 등의 과제는 높게 나왔다. 적정성 결정에 따른 기업내의 대응 과제에 대한 전체적인 과제의 평균값은 과제의 필요성 측면으로 판단했으며, 적정성 결정 전 · 후 모든 과제가 평균값 3.5 이상으로 기업에서 대응해야 하는 필요한 과제로 판단 할 수 있다.

또한 대응표본 t 검정을 실시한 결과에서 적정성 결정에 따른 과제의 중요성 변화 차이에 대한 결과로 '개인정보 범위, 흐름, 처리 유형 파악' 과제와 'DPA 계약서 준비 및 체결' 과제가 중요도 변화 차이가 있다고 나타났다.

Table 4. Comparison result of the importance of companies's task

Task	Average		t(p)
	Before	After	
Organize GDPR TFT	4.39	4.33	0.442(0.662*)
Identify the status of the EU Target system	4.69	4.45	1.606(0.118*)
Define Personal data Flow, Processing Type	4.63	4.42	2.235(0.033*)
Designation of the DPO	4.09	3.97	0.780(0.441*)
Data Protection by Design	4.33	4.24	0.620(0.540*)
Appropriate security & Personal data protection measure	4.36	4.27	0.902(0.374*)
DPA Prepare and Contract	4.39	3.55	3.815(0.001*)
Update IT System Improvements	4.06	3.82	1.606(0.118*)
Data Protection Impact assessment	4.09	3.94	1.000(0.325*)
Set Up and implement of Personal data breach procedure	4.24	4.00	1.543(0.133*)
training / Awareness	4.27	4.24	0.255(0.801*)

***p<.05, * *p<.01, * * *p<.001**

이외, 추가 조사 의견으로 'GDPR 이해를 위한 구체적인 가이드라인 필요', '기업별 규모에 맞게 최적 수준의 대응가이드를 통한 기업에서 자발적으로 개인정보보호 체계를 만들 수 있도록 정부차원의 선도적 지원 필요', '기업의 GDPR 이행에 따른 인증 및 공시 필요', '정부차원의 GDPR 관련 전담 조직 운영 필요' 등과 같은 정부차원의 GDPR 을 위한 차별화된 관리 방안이 필요하다는 결과를 포함했다.

V. 결론

EU 의 GDPR 이 법제화 되면서 정보주체의 권리 강화, 개인정보 처리자의 책임성 강화, 위반시 높은 징벌적 과징금 및 지리적으로 GDPR 적용 범위가 확대 되었다. 국내 기업이 EU 진출시에 개별로 GDPR 준수를 위한 EU 개인정보에 대한 적절한 보호조치 준비를 해야 한다. 이에 기업에서 필요한 과제를 단계별로 도출하였고, 정부차원에서 대응 중인 적정성 결정에 따른 개인정보 역외 이전에 대한 비용-편익과 과제 중요도 변화에 대해서 살펴보았다.

본 논문에서는 EU 거주민의 개인정보 역외 이전에 따른 기업의 준비 사항을 표준데이터보호조항을 참고하여 준수 되어야 할 과제를 '준비→GAP 분석과 개선방안 수립→적용' 단계별로 정의하였다. 또한 적정성 결정 이후 기업은 개인정보 보호조치에 대한 근거 마련과 EU 진출국가와의 계약 체결 준비가 생략되며 개별기업은 EU 와의 별도 대응준비가 필요 없어지게 된다. 이로 인해서 기업 규모에 따른 대응력의 차이 해소 및 준비를 위한 인적 · 물적 비용, 심사비용, 계약체결 비용등이 절감 되며, DPA 준비에 대한 절차 생략으로 인해서 적시에 EU 진출에 따른 기업 경쟁력 강화에도 도움이 되는 편익 증대 효과를 가져온다. 그러나 적정성 결정 이후에도 기업에서의 개인정보 처리자의 원칙에 대한 규제 준수는 변함이 없이 기업의 몫이며 개인정보 보호에 대한 강화 활동에 대해서는 지속적으로 유지가 필요하다.

이번 논문에서는 적정성 결정에 따른 기업 경제적 효과, 편익 증대의 영향에 대한 실증적 검증을 못한 한계가 있으며, 적정성 결정 후 정부의 구체적인 GDPR 대응 계획과 실질적인 기업의 과제에 대한 변화 연구 및 검증이 필요하다고 본다.

마지막으로 현재 정부에서 진행중인 적정성 결정이 완료가 되면 우리 나라 개인정보보호법제의 위상을 전세계에 알릴 수 있으며, 대외적으로 국내 기업들은 EU 시장에서 기업 경쟁력 확보가 가능하며, 대내적으로는 개인정보보호 체계 유지와 안전 이상 수준 유지를 위한 노력 또한 아끼지 않아야 한다.

VI. 참고문헌

[1] Article 29 Data Protection Working Party. "Guideline on Data Protection Officers(DPO)". European Commission, 2016.
[2] Enews-Today, https://www.enewstoday.co.kr/news/articleView.html?idxno=1473111,2021.
[3] European Commission., reform of EU data protection rules. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en, 2018.
[4] European Data Protection Board, "1 Year GDPR-taking stock," https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en, 2019.
[5] HanGukilBo, https://www.hankookilbo.com/News/Read/201911121483070582, 2019.
[6] I. S. Ham, "Legal Issues on the Cross-Border Transfer of Personal Data-Focusing on the EU-Japan Adequacy Decisions and Their Implications," Jeon-Nam University, 2019.
[7] ICO, GDPR preparation for Small organisa-tions. https://ico.org.uk/for-organisations/business
[8] A. R. Jung, "Review of requirements for transborder flow of personal information," Public Law Journal, 20(2), pp. 209-244, 2019.
[9] H. Jung, "Korean Companies response to the implementation of General Data Protection Regulation," PIS FAIR, 2018.
[10] KISA, "Report on the effectiveness of the EU's approval of adequacy and its analysis summary," 2018.
[11] KISA, MOIS, "GDPR Primary Guidelines for Korean Companies," 2017.
[12] H. Kim, and K. Lee, "A Study on the Legislative Proposal for EU GDPR Adequacy Decision," Seoul National University, 2019.
[13] T. H. Oh, M. J. Kang, "EU GDPR fermentation : assessment and response measure," KIEP World Economy today, 18(19), 2018.
[14] H. J. Park, J. H. Yang, "Issues of Adequacy Decision of GDPR and Policy Responses," Korea Institute Of Communication Sciences, 44(5), pp. 983-991, 2019.
[15] PrivIQ, https://priviq.com/?s=Technical+and+Organisational+Security
[16] Ruth, Boardman/James Mullock/Ariane Mole, Bird & Bird & guide to the General Data Protection Regulation, pp. 5, 2016.
[17] Y. H. Son, S. Son, "Korean Companies Response to the EU General Data Protection Regulations(GDPR)," The Journal of Comparative Private Law, 26(1), pp. 413-452, 2019.

저자 소개

김영수(YoungSoo Kim)

2021 년 6 월 중앙대학교 대학원 융합보안학과 석사과정

관심분야 : 개인정보보호, 정보보호, 산업보안

장항배(Hangbae Chang)

2006 년 연세대학교 정보시스템 박사
2014 년 ~현재 중앙대학교 산업보안학과 교수

관심분야 : 클라우드, 정보보호, 산업보안