Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.4, Aug. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.4.1013

국경간 개인정보 이전 규제에 대한 개선방안 연구: EU사례를 중심으로*

이 상 혁,† 김 인 석‡
고려대학교 정보보호대학원

A Study on Transborder Data Flow of Personal Information: Policy Suggestion based on EU's Approach*

Sang-Hyuk Lee,† In-Seok Kim‡
Center for Information Security Technologies(CIST), Korea University

요 약

국내 현행법상 개인정보 국외이전은 정보통신망법과 개인정보보호법에서 정보주체의 동의하에 국외이전을 허용하여 왔다. 하지만 최근 IT기술의 발달과 더불어 다국적 기업들의 국내 진출, 클라우드 활성화, FTA 협정 등을 통해 국가간 개인정보이전이 증가하는 가운데 현행 규제는 개인정보 국외이전에 뚜렷한 방향성을 제시하지 못한다. 개인정보의 국외이전 활성화는 국제협력 강화와 개인정보의 유통을 기반으로 하는 금융, 인터넷, 전자상거래 등 다양한 산업의 발전에 기여하는 바가 크며, 변화하는 정보통신기술 환경에 필수적인 요건이다. 따라서 개인정보의 보호의 원칙을 고수하며 개인정보의 해외 이전에 유연하게 대처하기 위해서는 새로운 개인정보이전 체계 마련에 대한 논의가 필요하다. 본 연구는 현행 개인정보 국외이전 법규의 한계와 새로운 제도의 필요성을 검토하고, 유럽의 개인정보 국외이전 사례 분석을 통해 정책 대안을 제시한다.

ABSTRACT

Transborder data flow(TBDF) of personal information in Korea has been limited by current Privacy law which request data subject to give consent. As the IT industry is growing at an incredible rate, there is a need to review the existing law to cope with growing industrial demand and increasing numbers of international data transfer. The transfer of personal data overseas not only allow businesses providing IT services including finance, internet, e-commerce to thrive, but also impact every aspect of our lives which are increasingly depended on these technology. Transmitting personal data across borders raises serious questions of privacy protection and restriction of business operation. In ordrer to promote interoperability of personal data in international environment, a considerable amount of research and debate needs to be taken before implementing a sound policy. This paper presents a need for a sound TBDF policy in Korea by examine the main policy challenges associated with TBDF. Finally, the paper identify policy suggestions based on European Union's approach as they have successfully implemented TBDF policy that balanced data privacy and economic agenda.

Keywords: Cross-border transfer, Privacy Act, International Data Transfer, Transborder Data Flow, EU Transfer

Received(06. 21. 2016), Modified(08. 02. 2016), Accepted(08. 03. 2016)

* 본 연구는 미래창조과학부 및 한국인터넷진흥원의 "2016년 고용계약형 정보보호 석사과정 지원사업"의 연구결과로 수행되었음

† 주저자, icnleesang@korea.ac.kr
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

I. 서 론

2016년 3월 발간된 맥킨지글로벌인스티튜트 '디지털 세계화' 보고서에 따르면 2014년 세계 GDP가 국가간 교역을 통해 10%(7조 8000억 달러) 증가하였다고 분석하였으며, 이중 2조 8000억 달러가 데이터 교역으로 이루어져 상품교역을 앞섰다 보고했다. 이는 실물상품의 이동위주로 이루어졌던 국제무역이 데이터 이동으로 변화되는 과정으로, 향후에는 지식·정보를 담은 무형자산의 거래가 국제무역을 주도할 것이라 예견하였다[1]. 핀테크 발달로 금융 거래가 쉬워지고, 고객수요 맞춤형 서비스나 정보 관련 부가가치산업 발달로 인해 개인정보를 포함한 데이터 유출입 또한 증가할 것으로 전망된다.

핀테크, IoT, 클라우드, 전자상거래 등 정보통신기술을 기반한 산업의 데이터활용은 필수적이다. 개인정보 국외이전은 이러한 산업육성에 필요한 개인정보를 자유로이 유통하여 기업들의 국제경쟁력 강화와 소비자의 편익증진으로 이어지게 하는 역할을 함으로써 그 의미하는 바가 크다.

우리나라는 지금까지 비교적 높은 수준에서 역내 개인정보가 다른 국가로 이전되는 것을 엄격히 규제함으로써 개인정보 역외 유출을 방지하는 조치를 취해왔다. 하지만 현행법은 정부가 현재 시행하고 있는 정보기술 활성화를 도리어 저해하고 정보기술산업의 변화 기조를 역행함으로써 그 실효성에 있어 괴리가 발생한다.

개인정보 국외이전에 대해 강력한 규제도 바람직하지 않지만 국외에서의 개인정보 침해 가능성 또한 무시할 수 없기 때문에 충분한 사례연구와 논의를 통해 장기적인 관점에서 표준화된 기준을 마련해야 한다. 본 연구에서는 개인정보 국외이전 현행법의 변경 필요성을 제시하고, 유럽의 개인정보 국외이전 사례 분석을 통해 정책 대안을 제시한다.

II. 개인정보 국외이전 현황과 새로운 제도의 필요성

2.1 디지털 환경변화

개인정보의 국외이전의 문제가 크게 제기되는 것은 갈수록 다변화되는 디지털 환경에 그 원인이 있다. 개인정보를 수집하는 디바이스가 증가하고, 이를 처리·유통할 수 있는 기술들이 발달함에 따라 개인정보를 국외가 쉽게 이전 될 수 있는 경로가 다양해졌다[2]. 반면에 이를 관리감독 할 수 있는 제도나 기준 마련은 상대적으로 미비한 실정이다. Table 1.은 개인정보를 수집 및 활용하는 외국 사업자의 현황과 예를 보여준다. 기술발전으로 인해 급격히 늘어나는 개인정보 국외이전은 이미 피할 수 없는 사항이며, 이용자들 또한 개인정보가 다른 나라에서도 안전하게 보호받을 수 있기를 희망할 것이다. 이러한 현실을 반영해보았을 때 우리나라 국민의 개인정보가 해외에서도 안전하게 유통될 수 있는 방안을 마련할 필요가 있다.

Table 1. Flow of Personal Information in Innovative Sectors

Business Sectors	Details
Manufacturing Sector	IoT devices such as Smart TV, Smart Watch (e.g. Apple Watch), and Heavy Machinery (e.g.: Komatsu) gather and process data across national borders
E-Commerce	Global e-commerce companies like Amazon, Alibaba, eBay gathers information of consumers and sellers worldwide for exchange of goods & services
Cloud Computing and Big Data (Outsourcingof Services)	Transfer and store large volumes of data from various sectors of business (finance, medical, etc.) for business operation cost, efficiency etc. Big Data analysis can be performed in outsourced companies in foreign country
Sharing Economy / App Economy	Small and Medium Enterprises are now able to market and distribute goods and services globally via online, gathering user information in the process. Sharing economy like Uber, AirBnb, KickStarter also gather and utilize personal information around globe
Multimedia and other services	Digital contents such as VOD, streaming services (e.g.: Netflix) and gaming content providers

2.2 자유무역협정의 확대

우리나라는 2004년 한국-칠레 자유무역협정(FTA) 발효를 시작으로 싱가포르, 유럽연합, 미국 등 14개 국가(2016년 6월 기준)와의 FTA를 발효시켰다. 현재 한중일, 중미6개국, 역내 포괄적 경제동반자협정(RECP) 등 다자간 자유무역협정 또한 협상 중에 있어 다른 국가들과의 협정을 통한 무역자유화는 지속될 것이다[3].

그러나 FTA 협상문 중에는 정보 이전에 관련한 내용이 포함되어 국내법과의 충돌 소지가 발생한다. 일례로 한-미 FTA에는 외국계 금융기업들이 우리나라 내 개인정보를 해외로 이전하여 관리할 수 있는 내용이 담겨 있다. 한미FTA 협정문 13장 제 2절 정보의 이전을 보면 "각 당사국은 다른 쪽 당사국의 금융기관이 그 기관의 일상적인 영업과정에서 데이터 처리가 요구되는 경우 그러한 처리를 위하여 자국 영역 안과 밖으로 정보를 전자적 또는 그 밖의 형태로 이전하는 것을 허용한다."라고 명시되어 있으며, 제3절 데이터 처리에 관련한 주석에는 "제2절에 따라 자국 영역 밖으로 정보의 이전을 허용할 의무를 지는 한도에서, 그 당사국은 또한 이전 후 그 정보의 데이터처리를 허용한다."라고 규정하였다[4]. 이는 금융회사가 보유하고 있는 개인정보, 금융정보를 미국으로 이전하여 처리 할 수 있는 법률적 근거를 제시한다. FTA 발효 당시, 금융회사들은 금융감독규정의 위수탁금지규정에 따라 금융사 내 해외 위탁이 불가능했을뿐더러 자국민의 금융정보의 해외이전 허용방안은 큰 논란을 불러일으켰었다[5].

FTA는 헌법상 국회 비준으로 법률적 효력을 갖게 되기 때문에 현행 법률과의 충돌을 피할 수 없으며 관련법의 개정이나 폐지가 불가피하다. 우리나라가 법률상 구체적인 개인정보 국외이전의 기준을 갖추지 못한다면 앞으로 체결될 FTA협정뿐만 아니라 여러 국가가 참여하는 다자간협정 협상과정에서도 개인정보 이전에 관련한 논란에 휩싸이기 쉽다.

2.3 개인정보보호법 및 정보통신망법

개인정보의 국외이전 관련 규정은 개인정보보호법 17조 3항과 정보통신망법 제63조에 개인정보주체의 사전동의를 통해서만 개인정보 국외이전이 허용되도록 요건이 설정되어 있었다[6]. 이는 자국민의 개인정보가 국외이전을 통해 유출될 수 있는 사고를 억제하는 장치로써의 그 역할을 해왔으나, 원칙적으로 개인정보 국외이전을 금지하지만 예외조항을 둔 유럽연합의 기준보다도 더 강력한 제한 규정이었다. 특히 대량의 정보를 처리·저장하는 클라우드와 빅데이터 기업입장에서 개인정보가 국경을 넘을 때마다 정보주체에게 별도의 동의를 얻는다는 것은 사실상 불가능하다. 이용자 또한 서비스 이용 시 국외이전 동의를 형식적인 옵트인(opt-in) 으로 인식하기 쉬우며 이미 동의를 받아 빠져나간 개인정보의 사후관리는 어려운 실정이다.

2016년 3월 정부는 제도의 유연성 확보 요구와 클라우드 활성화 정책을 반영하여 개인정보 국외이전과 관련된 조항을 일부 개정하였다. 새로 시행될 정보통신망법 제63조 제2항, 제64조의3제1항제8호의 신설된 사항과 그에 따른 영향은 다음과 같다:

- '이전'을 '제공(조회되는 경우를 포함), 처리위탁, 보관'으로 명시하여 '이전'의 범의 및 정의 획정
- 이용자의 동의를 없이 개인정보를 국외 이전하는 자에 대하여 매출액의 100분의 3 이하의 과징금을 부과하여 국외이전에 대한 규제강화
- 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우, 고지나 전자우편 등의 방법에 따라 이용자에게 알린 후에는 동의절차를 거치지 아니할 수 있게 함

이번 정보통신망법 개정은 동의절차를 거치지 않아도 이용자에게 고지를 통해 개인정보 국외로 처리위탁·보관할 수 있다는 점에서 기업들의 부담을 일부 경감시켰다. 그러나 개인정보 국외이전의 경우 규제강도가 낮은 상태에서 유출될 가능성이 높아진다는 점, 민감한 정보와 일반적인 정보에 대해 보안정책이 다르게 적용되야한다는 점, 명확한 원칙에 기반한 표준 마련이 필요하다는 점을 고려해 개인정보가 이전 후에도 안전하게 관리 될 수 있는 장치는 마련되지 않은 실정이다.

III. 기존연구 동향

국내 개인정보 국외이전 관련 연구들은 크게 법·제도 변경 및 국제협력 강화에 바탕을 두어왔다. 특히 한-미 FTA로 인한 개인정보 이전의 보안이슈와 클라우드·빅데이터 도입문제를 중심으로 논의가 지속적으로 이루어져왔다. 각 연구들을 살펴보면 먼저,

이정훈, 박석훈, 임종인 (2011)와 김은미(2013)는 FTA 체결에 따른 금융정보 국외이전에 안전한 보호책으로 제도적·기술적 방안마련이 필요하다고 보았다[7][5]. 박완규(2012)는 클라우드 컴퓨팅 환경에서의 개인정보의 이전의 문제를 지적하고 세이프하버(Safe Harbor) 협정 마련, 이용자의 개인정보보호 책임을 강화 등으로 리스크를 줄이는 방안을 제시했다[8]. 구태언(2013)은 개인정보의 국외이전 제한에 따른 산업 발전 저해를 강조하고 현행법률 개정, 정보주체 동의 철회권 보장, 개인정보 국외이전 내역 통보 등의 보안책 마련을 강조하였다[6]. 같은 맥락에서 한국인터넷진흥원(2015)은 개인정보 국외이전에 관한 예외적인 허용요건을 넓힐 수 있는 입법방안을 모색, 미국과 유럽연합이 체결한 세이프하버나 기업과의 BCR(Binding Corporate Rules)같이 개별 정보주체의 동의가 없어도 개인정보를 적법하고 안전하게 이전하여 처리할 수 있는 방안을 해결책으로 제시하였다[9].

각 연구들에서 동일하게 주장하는 바로는 개인정보 국외이전에 대한 구체적인 기준이 제시되어야 한다고 보았으며 이를 위해 새로운 제도 도입 및 기존 법률 정비, 기술적 보호관리, 세이프하버 같은 국가간 협정을 통한 종합적인 대책을 요구하였다. 하지만 세부적인 실행대책과 기준설정은 논의되지 아니하였다.

IV. 개인정보 국외이전 정책에 대한 이해

개인정보 국외이전 대안 제시에 앞서 개인정보 국외이전의 안전한 활용을 위한 필수 요건들과 국제 사례를 알아보고자 한다. 이는 대안 제시 시 예상되는 침해요인을 해소하고 국외이전의 허용 기준을 확립할 수 있는 기초 자료가 된다.

4.1 개인정보 국외이전 침해요인

개인정보 국외이전에서 발생 할 수 있는 침해요인들은 다음과 같이 정리할 수 있다[10]:

- 개인정보보호 수준이 약한 나라로의 이전되는 경우 침해 위험성
- 개인정보 물리적 위치 확인 문제
- 해외에서 자국민의 개인정보통제권이나 프라이버시권 보장의 어려움
- 유출·침해사고 시 책임, 보상, 처벌에 대한 협조
- 법 집행 기관에 의한 임의 접근 가능성
- 국가 간 다양한 법률 및 적용문제

개인정보보호 수준이 미흡한 국가로 자국민의 개인정보가 이전되는 경우 적절한 보호를 기대할 수 없으며 법제 또한 상이하여 개인정보의 침해 위험성이 커진다. 또한 당국의 관리 감독하에서 벗어난다는 점에서 정보주체의 권리행사가 어렵고 침해 후 보상이나 책임에 대한 문책이 이행되기 힘들다. 이러한 문제들을 토대로 개인정보 국외이전 대하여 다음과 같은 정책 근간이 도출되었다[11]:

1. 개인정보보호법와 데이터 보호법을 우회할 수 없도록 예방
2. 개인정보가 이전된 국가에서 데이터 처리 시 문제가 생기지 않도록 조치
3. 개인정보가 이전된 국가에서 데이터 보호와 프라이버시권 행사 어려움 해결
4. 소비자와 국민의 신뢰 향상

위와 같은 위험요소 및 정책 근간이 고려되어야만 개인정보가 역외이전 후에도 안전하게 관리될 수 있는 법적 체계가 마련될 수 있다.

4.2 유럽연합(EU) 개인정보 국외이전 제도 사례

유럽연합은 원칙적으로 개인정보 국외이전을 금지하지만 예외 장치를 둠으로써 유연성을 확보하였다. 이러한 안전장치들은 높은 수준의 보호를 보증함과 동시에 개인정보 국외이전의 장애물을 제거하여 경제활동을 촉진하려는 복합적인 목적을 반영한다.

EU 개인정보 보호지침 제25조1항에는 "제3국이 적정한 보호수준을 보장함을 제외하고는 유럽경제지역 이외에는 개인정보 이전을 금지한다"라고 규정되어있다. 그러나 개인정보 이전을 요구하는 국가나 기업이 적정한 보호수준을 보장하지 않더라 하더라도 각종 안전조치를 마련한다면 EU회원국의 개인정보보호 감독기구로부터 승인 받아 허용할 수 있는 조치를 두었다. 유럽연합의 개인정보 국외이전 허용 요건들과 흐름도를 Fig.1.과 Table 2.같이 정리하였다.

특히 "적정성 평가"는 역외국가가 EU개인정보보호지침에서 요구하는 수준으로 개인정보가 보호되고

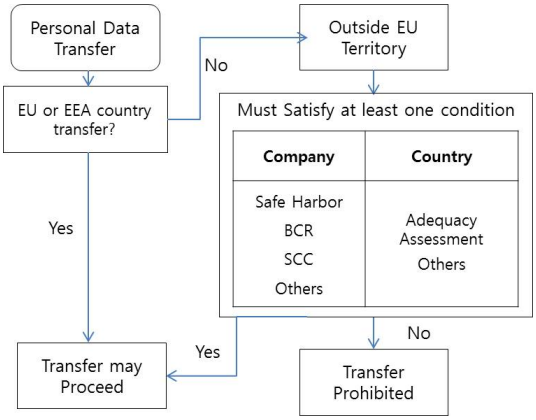

Fig. 1. EU Personal Data Transfer Decision-making Process

Table 2. EU Personal Data Transfer Mechanisms

Mechanism	Explanation
Adequacy Assessment	Transfer of personal data is allowed to non-EU country, if the country ensures an "adequate level of protection" approved by commission
Safe Harbor* (Invalid in Oct 2015)	Transfer of personal data for commercial purposes from companies in the EU to companies in the U.S. is allowed, if U.S. company has signed up to the Principles
Binding Corporate Rules (BCR)	Transfers of personal data within a multinational corporate group, which are approved by national Data Protection Authorities (DPA)
Standard Contractual Clauses (SCC)	With companies across the Atlantic, it specify data protection obligations and are approved by the Commission

있는지를 평가하는 제도로, 현재 스위스, 캐나다, 이스라엘, 아르헨티나 등 11개국이 평가 승인을 받았으며 가입국가의 기업들은 EU 기업들과 같은 기준으로 유럽시민의 개인정보를 자국으로 이전하여 활용할 수 있다. 우리나라 정부 또한 2015년 하반기부터 행자부 주도하에 'EU개인정보 보호수준 적정성 평가'를 추진하여 추가적인 보안대책 없이 유럽의 개인정보를 국내 기업으로 이전할 수 있는 방안을 모색하고 있다[12]. 적정성 평가 승인은 유럽집행위원회에서만 내릴 수 있으며 적정성 평가 시 고려되는 사항은 EU 정보보호법(Data Protection Directive) 제25조 2항에서 찾을 수 있다[13]:

- 정보의 성질(the nature of the data)
- 예정되어 있는 처리작업의 목적과 기간 (the purpose and duration of the proposed processing operation or operations)
- 정보 송신국과 최종 수신국 (the country of origin and country of final destination)
- 당해 제3국에서 유효하게 시행되는 일반적 분야별 법규범 (the rules of law, both general and sectorial, in force in the third country)
- 제3국에서 시행되는 전문적 법규범과 보안조치 (The professional rules and security measures which are complied with in that country)

일반적으로 개인정보 국외이전으로 인한 위험(Risk)와 정보주체권리(Rights of the data subject) 침해 가능성이 높을수록 법률적으로 더욱 철저한 심사를 받는다.

유럽연합의 적정성 평가나 세이프하버 협정은 국가간의 역외이전을 허용하는 선구적인 사례로 지목된다. 이 밖에도 구속력 있는 기업 규칙(Binding Corporate Rules)이나 표준계약조항(Standard Contractual Clauses)은 개별 정보주체의 동의가 없어도 EEA 영토 밖에 위치한 해외기업이 개인정보를 적법하고 안전하게 유통할 수 있는 선택권을 보장하였다.

V. 현행 유럽연합(EU) 개인정보 국외이전 제도에 대한 분석 및 문제점

국내 학계에서는 위와 같은 유럽연합의 개인정보 역외이전 제도 수용에 대해 긍정적 목소리를 높여왔다[5][7][8][9]. 하지만 대안으로 제시되는 유럽연합의 현행제도 또한 중대한 결점을 가지고 있어 이러한 문제점들을 분석해보고 개선책을 도출해보고자 한다.

5.1 적정성 평가 (Adequacy Assessment)

EU정보보호법의 "적정한 보호 수준"의 정의가 뚜렷하게 제시 되지 않은 가운데 유럽연합국 이외 제3

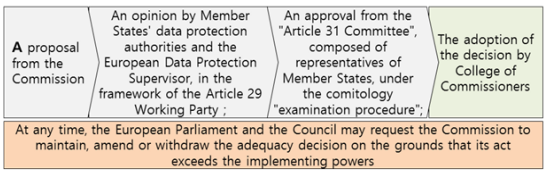

Fig. 2. Procedure for EU Adequate Level of Protection Assessment of Third Country

국이 적정성 평가를 받으려면 복잡한 판정절차를 거쳐야 한다[14]. 이는 각국이 통일된 기준의 정보보호 체계를 가지고 있지 않아 절대적인 기준을 적용하기 어렵기 때문이다. 이를 감안하여 적정성 평가 시에는 EU 정보보호법 제25항의 고려사항뿐만 아니라 사례별 접근방법 (case-by-case approach), 융통성 있고 개방적인 접근방법 (flexible and open approach), 그리고 기능적인 접근방법(functional approach)을 통해 해당국의 전반적인 정보보호수준, 법규, 기술적 조치, 기본원칙 반영 등 다방면을 분석하여 판단한다[15].

EU의 적정성 평가는 심사절차(Fig.2.)가 까다롭고 평가과정 어느 시점에서나 집행위원회가 인정을 보류하거나 불인정 할 수 있다. 더욱이 심사국의 주관적인 평가가 일부 반영될 수 있어 공정성 문제가 제기될 수 있다. 일례로 이스라엘은 2010년 하마스 요인 암살에 쓰인 영국과 아일랜드 위조여권 사건에 연루되어 양국의 반대로 최종단계에서 심사가 보류된 적이 있었다[15]. 하지만 유럽당국은 이러한 문제들을 감안하여 절차의 투명성을 강화하였고 평가받은 국가에 대해 집행위원회의 판정과 개인정보보호작업반(working party)의 견해를 공식적으로 게재하여 공정성을 확보하려는 노력을 보였다.

5.2 세이프하버 협약

개인정보 국외이전 시 가장 문제가 되는 요소는 각국의 개인정보보호 수준과 법률이 상이하다는 것이다. 정보유통의 자유를 통해 상업적 가치를 추구하는 미국과 엄격한 권리 보장을 추구하는 유럽연합만 보더라도 그 배경에는 상충적인 가치를 내포하고 있다. 이는 각국이 개인정보의 대해 다른 수준의 개념, 철학, 규제를 가지고 있기 때문인데, 이를 통일시킬 국제적 기준이나 제도 수립은 어려운 수준이다[16]. 유럽과 미국은 2000년도 세이프하버 협약을 체결하여 충돌하는 양국 법의 조화를 이루려고 하였으나, 2015년 10월 유럽연합사법 재판소의 무효화 판결(Maximillian Schrems v. Data Protection Commissioner)에서 볼 수 있듯이 체결국(미국)의 법률이 당국(EU)의 보호수준을 법적으로 강제하지 않을 경우 절충된 성격의 협약이 지속될 수 없다.

미국의 경우 유럽연합 같은 포괄적인 개인정보보호 법안이 부재한 상태에서 세이프하버 협약을 추진했었다. 당시 미국상무부(US Department of Commerce)는 2년간의 노력 끝에 자율 규제 체계를 만들어 美기업들이 EU 정보보호법의 요구사항을 만족시킬 수 있는 대안을 내놓았다. 이에 EU의 개인정보 이전을 원하는 기업들은 세이프하버에서 요구하는 고지정책, 선택권 부여, 재이전의 제한, 접근권한, 안전조치, 정보의 무결성 관리, 집행의무 등의 인증 얻어 미국의 공정거래기구(FTC)의 관리감독을 받게 되었다[10][13].

세이프하버는 OECD 8원칙과 유럽연합의 적정성에서 요구하는 사항을 반영하여 그 원칙에는 문제가 없었다. 다만 이를 이행하고 관리감독하는 과정에서의 사건이 빈번히 발생했다. 세이프하버 가입 기업들 중 상당수가 세이프하버에 입각한 개인정보보호방침(Privacy Policies)을 공개하지 않았고, 가입인증을 주장하는 기업 중 10%가 현 구성원에서 탈락된 기업으로 밝혀지는 등 협약이 유지되는 기간동안 관리소홀에 대한 불신을 낳았으며 2013년 에드워드 스노든의 미 국가안보국(NSA)의 무차별한 통신 수집 행위 폭로로 프라이버시 침해가 사실화되면서 15년간 유지되었던 협약은 그 끝을 맞게 되었다[10][13][14].

세이프 하버는 상충하는 개인정보보호법제를 가진 두 국가가 합의아래 개인정보 국외이전의 혜택을 볼 수록 있게 한 대표적 예다. 하지만 일괄적인 개인정보보호법이 시행이 되지 않는 국가에서 동일한 개인정보보호 수준을 보장받으려면 기업의 기준 준수와 해당국의 관리감독 체계에 대한 투명성이 제고되어야만 한다.

5.3 구속력 있는 기업 규칙(Binding Corporate Rules)

구속력 있는 기업규칙(BCRs)은 EU 역내에서 사업활동을 하는 기업그룹이 그룹 내부의 정보교류 시 EU 개인정보보호원칙을 준수할 것임을 확약하고 정보주체의 각종 권리구제수단을 정해놓은 행동강령

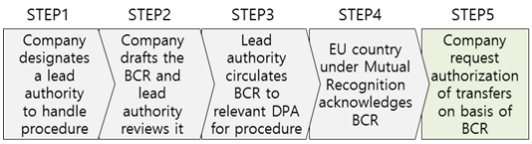

Fig. 3. Procedure for Authorization of BCR

(Code of Conduct)을 지칭한다[15]. BCRs는 주로 다국적 기업이 그룹 내부에서 정보를 이전하는 경우에 한하여 적용되며 EU의 적정한 보호수준을 갖추지 못한 제3국의 위치한 기업계열사라도 국외이전을 허용 가능하게 하였다.

EU 개인정보보호작업반이 BCRs를 도입한 배경에는 2가지의 목적이 있다. 첫째, 국제적인 정보 유통 촉진을 위해 규제를 간소화할 필요가 있다고 보았고, 둘째로 다국적기업이 EU지침에 맞게 개인정보보호 정책을 수용하고 전세계적으로 시행할 수 있도록 의도하였다.

BCRs의 기준은 상당히 자세히 명시되어있으며 반드시 포함해야 할 사항은 다음과 같다[15][17]:

- 정보의 흐름을 처리하는 것이 EU 개인정보 보호 지침에 부합하여야 함
- 내부적인 시행절차는 자가진단 및 감사, 규칙의 준수를 입증할 수 있는 정보주체에 대한 규칙 및 수단의 투명성, 불만 및 고충처리, 제재수단을 포함함
- 보고사항의 변경에 대한 메커니즘
- 구속력 있는 기업규칙을 대내외적으로 준수하기로 하는 책임이 계약서 등에 반영

개인정보보호 수준이 약하거나 입법 되지 않은 나라의 기업이 직접 표준화된 규칙과 승인절차를 밟아 정보보호 수준을 제고할 수 있다는 점에서 BCRs는 앞으로도 확대될 예정이다. BCRs은 내부정책의 유연성, 책임강화, 정보보호 수준제고, 홍보효과, 데이터보호국(Data Protection Authority)과의 관계개선 등 기업입장에서 상대적으로 많은 이점을 가지고 있는 반면에 이를 준비하고 승인하는 기간이 최소 12개월 이상 소요되며 이에 따른 비용 또한 만만치 않은 문제점을 가지고 있다[18].

VI. 대안 비교 및 개선사항

6.1 대안 비교분석

우리나라 법제상 개인정보 국외이전을 금지하는 이유는 자국민의 정보가 개인정보보호 수준이 약한 나라로의 이전되는 것을 방지하기 위함이며 개인정보보호 규제가 엄격하거나 동등한 국가·기업으로의 이전을 금할 이유는 없다. 원활한 개인정보 교류를 위해서는 규제완화보다는 EU처럼 적정한 보호수준을 가진 국가·기업의 개인정보 이전을 허용하는 방안을 마련해야 한다. 일방적인 규제완화는 개인정보의 침해 가능성을 높이는 반면, EU의 기준은 4.1에서 언급된 침해위험성을 경감시킬 뿐만 아니라 개별적인 사례에 맞추어 여러 옵션을 갖추었기 때문이다. 단, 이러한 기준을 도입하기 위해서는 각 안전조치의 장단점을 고려하고 이를 관리할 수 있는 적절한 기관과 자원의 배치가 우선시 되어야 한다. EU의 국외이전 안전장치들의 개요와 장단점 분석은 Table 3.와 Table 4.에 정리되었다.

먼저, 회원국의 개인정보 감독기구가 제3국의 적

Table 3. EU Personal Data Transfer Mechanisms

	Adequacy Assessment	Safe Harbor	BCRs
Type of Mechanism	Assessment / Evaluation	Agreement between two nation	Contractual
Beneficiary	Applicant country and organizations within	Organizations that abide by Safe Harbor rules	Multi-national companies or global organization
Level of Procedure	Long and cumbersome procedure	Easy to certify once meet given requirements	Straightforward but needs lots of preparation
Restriction on Onward Transfer	Not applied if country ensures adequate level of protection	Applied	Not applied within company and its branch
Time required Approval	2~4 years	2 years (in case of US)	1~# years (Getting shorter)

Table 4. Advantages and Disadvantages of EU Transfer Mechanisms

Mechanisms	Advantages	Disadvantages
Adequacy Assessment	-Increase in the level of information security by meeting EU standard -All organizations within the approved country are provided with same privilege	-Cumbersome procedure -No actual standard for assessment -Re-examination of current regulation -Prone to subjective judgment
Safe Harbor	-Gov't of recipient country sets out rules and monitor the companies -Companies can easily apply for Safe Harbor for the transfer of personal data -Alternative for the country without meeting the requirement of the adequacy assessment	-Individual company has no voice in negotiation -Financial organization are excluded -No onward transfer -May lead to lack of enforcement and appropriate management -May rise possible legal dispute
BCRs	-Suitable for multinational and global companies -Onward transfer within company -Clear standard and procedure -Alternative for Adequacy Assessment and Safe Harbor	-Not suitable for Small and Medium Enterprises -Long procedure in terms of time and upfront cost -Different rules for nature of industry and data

정한 보호수준을 심사하는 적정성 평가는 해당국가의 개인정보 보호 관련 법령, 실질적인 법·제도 운영 현황 등을 종합적으로 평가할 수 능력이 수반되어야 한다. EU의 경우 이를 담당하는 기관뿐만 아니라 30명 이상의 조사반까지 동원되어 체계적인 운영이 가능토록 하였다[12]. 또한 타국을 심사한다는 자격요건을 갖추려면 정보보호 선진국에 걸맞은 국제적 위상이 뒷받침 되어야 할 것이다.

세이프하버는 교역국가와의 협약을 통해 체결할 수 있다. 상대국이 우리나라 개인정보보호 수준에 부합하는 기준을 세워 이를 준수하고 집행할 수 있는 기관들을 협의 내용에 반영한다면 우리나라가 이를 고려해 허용하는 방안이다. 다만 EU의 세이프하버 무효화에서 볼 수 있듯이 이행과정 중 투명성이 보장되어야 하며 위반 시 우리나라가 제재를 가할 수 있는 법률적 권한이 지원되어야 한다.

BCRs도입 시 우리나라는 구속력 있는 기업규칙을 마련하여 글로벌기업을 심사할 수 있어야 한다. 이미 EU의 BCRs가 확대되는 시점에서 우리나라는 심사에 대한 절차나 사례를 벤치마킹 할 수 있을 뿐만 아니라 기존의 정보보호관리체계 인증제도(K-ISMS) 등의 역량을 갖추고 있어 상대적으로 수용이 수월할 것이다.

EU 사례에서 볼 수 있듯이 하나의 수단을 고집하기 보다는 여러 안전장치를 두어 개인정보 국외이전 신청 국가·기업이 최적화된 장치를 선택할 수 있도록 설정해야 한다. 이는 신청자와 평가자 모두 실정을 고려해 시간과 비용을 절약할 수 있어 원활한 진행이 가능해진다. 또한 EU의 세이프하버 무효화에서 볼 수 있듯이 유사 시 각 안전장치가 대체기능을 제공하여 피해기업이 손실을 최소화 할 수 있는 조치방안이 될 수 있다.

6.2 국제협력 강화

국제적으로 안전한 정보교류 환경을 만들기 위해서는 우리나라 국제위상을 높이기 위한 노력이 필요하며 그 이유는 다음과 같다:

- 주요국들의 개인정보 및 산업보호를 위해 자국민의 개인정보가 해외로 유출 되지 못하도록 규제를 강화하는 추세
- 국내기업들의 해외시장 진출 여건 개선 및 국제거래 증진
- 개인정보보호 선진국으로써의 도약과 국내 정보보호 기준의 세계화
- FTA 등 국제협정 테이블에서의 우위효과

개인정보 국외이전은 국가적으로도 민감한 문제이며 국제적인 공조 없이는 해결이 어렵다. FTA가 아시아태평양으로 확대되고 데이터 교역이 급격히 증가하는 시점에서 개인정보의 국외이전을 막기란 불가능하다. 특히 우리나라는 아시아 태평양 국가들과의 개인정보보호에 대한 이해차이가 크기 때문에 문제 발

생시 이를 해결하기가 어려운 실정이다[15]. 이들 국가와의 협상에서 우위를 점하려면 우리나라의 명확한 개인정보 이전 법률이 교섭의 준거틀로 원용되어야 하며 이를 기준으로 타협점을 찾을 수 있어야 한다.

정보보호선진국으로써의 국제적인 위상을 높이기 위해서는 먼저 우리나라의 정보보호 수준을 대외적으로 인정받아야 한다. 현재 우리나라가 추진 중에 있는 EU 적정성 평가와는 별개로 개인정보보호 법제의 모델이 되고 있는 유럽회의 협약 108호(CoE 108)에 가입을 신청하는 전략 또한 고민해볼 필요가 있다. 아울러 개인정보와 관련된 국제회의와 협의체에 주도적인 역할을 수행함으로써 각국과의 협력을 강화할 수 있도록 노력 하여야 한다.

6.3 프라이버시 쉴드의 등장

2016년 7월 EU와 미국은 세이프하버의 대안으로 2년간의 재협상 끝에 '프라이버시 쉴드(Privacy Shield)'를 최종 체결함으로써 기존의 투명성(transparency), 책임 (obligation), 감독(Monitoring)을 강화하였다. 세부적인 방안은 다음과 같다[19]:

- 유럽이 규정한 정보 보호 기준 준수 이행을 증명하는 '자기인증(Self-certify)' 매년 갱신
- 미국 상무부가 프라이버시 쉴드 가입 기업을 '적극적으로 감독·검증 (Monitor and actively verify)' 하여 미이행 기업에 대해 처벌 및 벌금 부과
- 정보주체의 민원을 45일 내에 처리하고 분쟁해결 기구의 운영으로 해당 문제를 원활히 대응
- 국가안보분야에서 유럽 시민들을 위한 배상 및 민원을 해결하는 '옴브즈맨(Ombudsperson) 제도' 도입

프라이버시 쉴드의 등장은 세이프하버의 문제점을 최소화하는 방안으로 서로의 협약을 매년 주기적으로 공동검토(Annual Joint Review)하고 엄격한 감시감독 프로세스 밟는 방안을 제시하였다. 이는 무효화 되었던 양국 개인정보이전 정책의 '신뢰'를 회복함으로써 세이프하버2.0의 시대를 열려는 취지를 반영했다. 프라이버시 쉴드의 향후 행보에 따라 국내 개인정보 국외이전의 정책 또한 새로운 국면을 맞게 될 가능성이 높다.

VII. 결 론

본 논문은 개인정보가 해외에서도 안전하게 유통될 수 있는 방안으로 EU의 사례를 분석하여 대안으로 제시하였다. EU는 개인정보 국외이전을 원칙적으로 금지하면서도 조건부에 한하여 개인정보를 역외로 이전할 수 있는 장치를 마련하였다. EU의 제도적 유연성은 자국민의 개인정보가 제3국에서도 보호될 수 있도록 보증할 뿐만 아니라 경제활동 촉진을 위한 장애요소를 제거하는 복합적인 목적을 달성하였다.

우리나라는 지금까지 개인정보 국외이전을 억제하는 정책을 고수해왔다. 하지만 이러한 자세는 변화하는 정보기술산업의 기조를 역행 할 뿐만 아니라 국제적 무대에서도 우리를 불리한 위치에 자리하도록 만든다. 따라서 우리나라도 충분한 연구 끝에 개인정보를 안전하게 유통할 수 있는 대안을 제시 할 필요가 있으며 동시에 국제 협력과 공조를 강화하여 정보보호 선진국으로써 국제적인 위상을 갖춰야 할 것이다.

향후 연구에서는 데이터의 국외이전 수요가 높은 클라우드 및 빅데이터 산업 중심으로 이전된 개인정보를 효율적으로 관리할 수 있는 기술적 조치에 대해 연구할 계획이다.

References

[1] http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx "Digital Globalization: The New Era of Global Flows," Mckinsey Global Institute, March. 2016.

[2] Usman Ahmed and Anupam Chander, "Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows," E15 Initiative by International Centre for Trade and Sustainable Development and the World Economic Forum, pp. 1-2, Feb. 2016.

[3] http://fta.go.kr/main/situation/fta/wo

rld "World FTA Status," Ministry of Trade, June. 2016.
〔4〕 http://fta.go.kr/us/doc/1/ "US-KOREA FTA Agreement Chapter 13," Ministry of Trade, 2014.
〔5〕 Eun-Mi Kim, "A Study on the Financial Service in KORUS FTA : Focused on TBDF for Financial Data," The Journal of Korea Research Society for Customs 14(2), pp. 107-131, May. 2013.
〔6〕 Tae-Eon Koo, "Status and Improvement of the Legal System about the Transfer of Personal Information Abroad," Gachon Law Review, 6(2), pp. 277-312, March. 2012.
〔7〕 Jung-hun Lee, Seok-hoon Park, and Jong-in Lim, "A Study on the policy counterplan of Cross Border Financial Information Transfer according to FTA," Journal of The Korea Institute of Information Security and Cryptology, 21(3), pp. 117-130, June. 2011.
〔8〕 Wan-Q Pak, "Solutions to Problems regarding Transfer of Korean Personal Information to the U.S. in the Cloud Computing Environment," Kyungpook National University Law 38, pp. 455-478, Feb. 2012.
〔9〕 Korea Internet&Security Agency, "The analysis and reaction plan for current situation about cross-border data transfer," KISA-WP-2016-0015, Dec. 2015.
〔10〕 Rolf H. Weber, "Transborder data transfers: concepts, regulatory approaches and new legislative initiatives," International Data Privacy Law, vol. 3, no. 2, pp. 117-130, Feb. 2013.
〔11〕 Christopher Kuner, "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future," OECD Publishing, no. 187, pp. 22-24, Dec. 2011.
〔12〕 http://www.moi.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=47865 "Level of Korea's Personal Data Protect Will Meet International Standard," Ministry of the Interior, Dec. 2015.
〔13〕 https://www.hoganlovells.com/en/~/media/ace8805a3cc04a308cadd47d3749f526.ashx "Legal Analysis of the EU-U.S. Privacy Shield," Hogan Lovells, March. 2016.
〔14〕 Marc Rotenberg and David Jacobs, "UPDATING THE LAW OF INFORMATION PRIVACY: THE NEW FRAMEWORK OF THE EUROPEAN UNION," Harvard Journal of Law & Public Policy, vol. 36, no.2, pp. 605-652, March. 2013.
〔15〕 Whon-il Park, Legal Issues and Solution to Personal Data Transfer, 1st Ed., Jipmoondang, Oct. 2015.
〔16〕 Seok Jin Lew and Woo Young Chang, "Transborder Data Flow and Dynamism of International Norms: Focusing on the Conflict between the EU-type andU.S.-type," Journal of International Area Studies, 9(3), pp. 79-117, Oct. 2005.
〔17〕 http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm "FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES," The European Commission, 2015.
〔18〕 http://www.allenovery.com/SiteCollectionDocuments/BCRs.pdf"Binding Corporate Rules," Allen & Overy LLP, Feb. 2013.
〔19〕 http://europa.eu/rapid/press-release_MEMO-16-2462_en.htm, "EU-U.S. Privacy Shield: Frequently Asked Questions," The Eureopean Commission, 2016.

〈저자소개〉

이 상 혁 (Sang-Hyuk Lee) 학생회원
2013년 8월: 한동대학교 국제법학과 학사
2015년 3월~현재: 고려대학교 정보보호대학원 금융보안학과 석사과정
〈관심분야〉 전자금융보안, 개인정보보호법

김 인 석 (In-seok Kim) 종신회원
1973년 2월: 홍익대학교 전자계산학과 학사
2003년 2월: 동국대학교 정보보호학과 석사
2008년 2월: 고려대학교 정보경영공학과 박사
1980년~2011년 : 한국은행, 금융감독원 근무
2011년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 전자금융보안, IT감사, 전자금융법규