법제현안분석지원 현안대응 2-⑦

# 해외이전 우리 국민의 개인정보 보호 방안 마련 연구

이 경 희 · 최 경 진

Korea Legislation Research Institute

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

# 해외이전 우리 국민의 개인정보 보호 방안 마련 연구

## A Legislative Study for Personal Data Protection of Overseas Korean National

연구책임자 : 이경희 부연구위원(한국법제연구원)
Lee, Kyunghee
최경진 교수(가천대학교)
Choi, Kyoungjin

2018. 11. 09.

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

## 연 구 진

| | |
|---|---|
| 연구책임 | 이경희 부연구위원 |
| 공동연구(원외) | 최경진 교수 (가천대학교) |
| 심의위원 | 현대호 선임연구위원<br>최 유 연구위원<br>이인호 교수 (중앙대학교) |

# 요 약 문

## Ⅰ. 연구의 목적과 범위

### ▶ 연구의 목적

○ 우리 국민의 해외에서의 개인정보보호에 관한 법제도 개선 방안 도출을 위한 기초 연구

- 해외 사례 연구
- 현행법 상의 규율 체계 및 문제점

○ 우리 국민의 해외에서의 개인정보의 효과적인 보호를 위한 법제도 개선 방안 도출

### ▶ 연구의 범위

○ 국제적인 논의동향으로서 자국민의 개인정보보호를 위한 개인정보보호법제 해외 사례 연구

○ 해외에서의 우리 국민의 개인정보 처리에 관한 현행법상의 규율 체계 및 문제점 분석

○ 해외에서의 우리 국민의 개인정보의 효과적인 보호를 위한 법제도 개선 방안 연구

## Ⅱ. 주요 내용

○ 우리 국민의 해외에서의 개인정보보호에 관한 글로벌 기준과의 조화를 위하여 국제적인 논의동향으로서 자국민의 개인정보 보호를 위한 개인정보보호법제 해외 사례 연구

- EU GDPR, 일본 등에서의 역외 개인정보처리에 대한 규율체계 비교 분석
- 해외에서의 데이터 국지화(data localization) 법제 분석
  (예, 중국, 러시아, 캐나다, 미국 등에서의 데이터 국지화를 위한 법제도 분석)

○ 해외에서의 우리 국민의 개인정보 처리에 관한 현행법상의 규율 체계 및 문제점 분석

- 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보보호법 등 현행 개인정보보호 관련법 하에서의 해외에서의 개인정보 처리에 대한 규율 체계 분석과 문제점을 분석하여 개선방안 도출의 근거 마련

○ 해외에서의 우리 국민의 개인정보의 효과적인 보호를 위한 법제도 개선 방안 연구

- 외국 입법례를 비교 분석하고, 우리나라에서의 개인정보보호에 대한 법제도 환경이나 법제도적 수요 등을 검토
- 우리 국민의 해외에서의 개인정보보호를 위한 바람직한 법제도 개선방안을 도출
- 외국과의 공조체계 구축 등 외국과의 협력방안 도출

## Ⅲ. 기대 효과

▶ **해외에서의 우리 국민의 개인정보보호를 위한 효과적인 대응체계 구축 및 관련 법제도 개선에 활용**

○ 향후 「개인정보 보호법」 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 개정에 활용

▶ **주제어 : 개인정보, 프라이버시, 개인정보보호, 해외 이전, 역외적용, 상호주의**

# Abstract

## Ⅰ. Purpose and Scope of Research

### ▶ Purpose of Study

○ Basic research for the improvement of legal system for the protection of personal information of foreign nationals

- Foreign case study
- Regulatory system and problems in current law

○ Study of improvement of the legal system for the effective protection of the personal information of the Korean people abroad

### ▶ Scope of Research

○ Study of foreign law system on the protection of personal information for the protection of personal information of the citizens

○ The regulatory system and problem analysis of the current law on the protection of personal information of the Korean people in foreign countries

○ Study on improvement of legal system for effective protection of personal information of the Korean national in foreign countries

## Ⅱ. Contents

○ Study of foreign law case in order to harmonize with the global standards for the protection of personal information of nationals in foreign countries

- Comparative analysis of regulatory system for personal information protection in foreign country with EU GDPR and Japanese
- Comparative legal analysis on 'Data Localization'
  (Eg, analysis of legislation for localizing data in China, Russia, Canada, and the United States)

○ The legal system and problem analysis of the current law on the protection of personal information of the Korean people in foreign countries

- Analysis of the protection system of personal information processing in foreign countries under the current personal information protection laws, such as the Personal Information Protection Act, the Promotion of Information and Communication Network Utilization and Information Protection Act, and the Credit Information Protection Act.

○ Study on improvement of legal system for effective protection of personal information of the people in foreign countries

- Comparing and analyzing foreign legislative cases and reviewing the legislative system for protection of personal information in Korea, according to the change of environment and legal institutional demand
- Making improvement plan for the desirable legal system for the protection of personal information of Korean nationals in foreign countries
- Establishing cooperation with foreign countries

## Ⅲ. Expected Effects

▶ Contributing to establish an effective response system for the protection of personal information of Korean nationals in foreign countries and utilize this report to improve related legal system

○ In the future, good reference for the amendment of the “Personal Information Protection Act” and the “Information Communication Network Promotion and Information Protection Act”

▶ Key Words : Personal data, Privacy, Personal data protection, Data protection, Extraterritorial application, Crossborder transfer, Principle of Reciprocity

CONTENTS

# 목차

# 목차

korea
legislation
research
institute

# 제1장
# 서 론

# 제1장 서 론

## 제1절 연구의 필요성 및 목적

### Ⅰ. 연구의 필요성

글로벌 ICT 환경의 변화에 따라 해외로 이전되는 우리 국민의 개인정보보호의 필요성이 증가하고 있다. 즉, 글로벌 ICT 환경의 변화로 인터넷이 연결되는 전세계로 우리 국민의 개인정보가 이전되어 처리되는 경우가 증가하고 있으며, 해외에서 국내로 서비스를 제공하는 사업자가 증가하고 해외 서비스를 이용하는 국민이 증가함에 따라 우리 국민의 개인정보와 관련한 권리를 보호할 필요성도 함께 증가하고 있다.

우리 국민의 개인정보가 해외로 이전된 경우, 국내 주권이 미치지 못하여 해외 공공기관에 의해 정보주체의 동의 없이 열람을 당할 우려가 상존하고 있다. 또한 해외 공공기관이 당해 국가의 법률을 근거로 정보 수집 기업에 대해 우리 국민 정보공개를 요청하거나 압수수색을 하는 경우도 발생할 수 있다. 해외 공공기관에 의해 열람된 우리 국민 개인정보가 제3국가로 유출되는 경우에는 추가적인 피해가 발생할 가능성이 있다. 이처럼 개인정보의 해외이전이 증가하는 추세에서 가칭 '디지털 치외법권' 설정을 통해 해외 공공기관의 무분별한 정보 열람을 방지할 필요도 있다.

해외 주요 국가의 입법적 측면에서도 자국민의 개인정보를 보호하려는 해외 입법례가 증가하고 있다. 자국민의 개인정보를 보호하여 데이터 주권을 지키고 국민의 기본적 자유와 권리를 보장하려는 시도가 증가하고 있다. EU, APEC, ICDPPC 등 다양한 국제기구에

서 개인정보의 보호를 위한 법규범이나 논의가 증가하고 있으며, 특히 EU는 2018년 5월부터 시행된 GDPR을 통하여 EU 역내 회원국 국민의 개인정보를 보호하기 위한 강력한 규정을 시행하고 있고, 해외로 이전되는 EU 회원국 국민의 개인정보보호를 위한 체계를 정립하고 있다. 중국이나 러시아, 캐나다 등 데이터 국지화(data localization) 관련 법제를 통하여 자국민의 개인정보를 보호하려는 노력이 증가하고 있다.

이러한 동향에 대응하여 우리 정부도 EU GDPR 적절성(adequacy decision) 평가를 추진 중에 있으며 그에 따라 해외에서의 우리 국민의 개인정보의 보호의 필요성도 함께 중요해지고 있다. 우리나라 기업이나 개인정보처리자가 EU 회원국 국민의 개인정보를 처리하는 과정에서 EU GDPR에 따른 적절한 처리를 할 수 있는 환경을 마련하기 위하여 우리 정부는 GDPR 적절성 평가를 추진하고 있으며, 연내 평가가 완료되도록 추진 중에 있다. GDPR 적절성 평가는 EU 회원국 국민의 개인정보보호를 위한 것인 만큼 그에 대응하여 우리 국민의 개인정보가 해외에서도 적절하게 보호될 수 있는 법제도적 환경 조성이 필요하다.

## Ⅱ. 연구의 목적

우리 국민의 해외에서의 개인정보보호에 관한 글로벌 기준과의 조화를 위하여 국제적인 논의동향으로서 자국민의 개인정보 보호를 위한 개인정보보호법제 해외 사례를 연구한다. 즉, EU GDPR, 일본 등에서의 역외 개인정보처리에 대한 규율체계를 비교 분석하고, 최근 개인정보보호를 목적으로 한 해외에서의 데이터 국지화(data localization) 법제를 분석하고자 한다. 예를 들면, 중국, 러시아, 캐나다, 미국 등에서의 데이터 국지화를 위한 법제도를 분석하고자 한다.

해외에서의 우리 국민의 개인정보 처리에 관한 현행법상의 규율 체계 및 문제점을 분석하여 개선방안 도출을 위한 기초연구를 하고자 한다. 즉, 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보보호법 등 현행 개인정보보호 관련법 하

에서의 해외에서의 개인정보 처리에 대한 규율 체계 분석과 문제점을 분석하여 개선방안 도출의 근거를 마련하고자 한다.

해외에서의 우리 국민의 개인정보의 효과적인 보호를 위한 법제도 개선 방안을 도출하고자 한다. 즉, 외국 입법례를 비교 분석하고, 우리나라에서의 개인정보보호에 대한 법제도 환경이나 법제도적 수요 등을 검토하고, 우리 국민의 해외에서의 개인정보보호를 위한 바람직한 법제도 개선방안을 도출하고자 한다. 또한 외국과의 공조체계 구축 등 외국과의 협력방안도 도출한다.

## 제2절 연구의 범위 및 방법

### Ⅰ. 연구의 범위

자국민의 개인정보 보호를 위한 개인정보보호법제 해외 사례 연구를 위하여 EU GDPR 상의 역외적용 및 역외이전 규율 체계 분석, 일본의 개인정보 역외이전에 대한 규율체계, 해외에서의 데이터 국지화(data localization) 법제 분석을 시도한다. 특히 데이터 국지화의 경우에 중국, 러시아, 캐나다, 미국 등에서의 데이터 국지화를 위한 법제도 분석을 실시한다.

외국인 개인정보 열람에 관한 해외 법제 조사를 통하여 해외 정부 및 공공기관이 자국에서 수집・보관된 또는 타국에 보관된 외국인의 개인정보 열람을 허용하는 해외 법 사례(예, 미국의 CLOUD법 등)를 살펴본다.

해외에서의 우리 국민의 개인정보 처리에 관한 현행법상의 규율 분석 측면에서 우리나라의 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 신용정보보호법 등 현행 개인정보보호 관련법 하에서의 해외에서의 개인정보 처리에 대한 규율 체계를 분석한다.

이러한 연구를 바탕으로 하여 해외에서의 우리 국민의 개인정보의 효과적인 보호를 위한 법제도 개선 방안을 연구하고자 한다. 즉, 외국 입법례를 비교 분석하고, 우리나라에서의 개인정보보호에 대한 법제도 환경이나 법제도적 수요 등을 검토한 후 우리 국민의 해외에서의 개인정보보호를 위한 바람직한 법제도 개선방안을 도출한다. 안전한 데이터 국외이전을 위한 상호운용 가능한 법적 협력방안으로서 개인정보 보호 분야에의 상호주의, 국제법상 원칙 등을 다각적으로 분석하고자 한다. 아울러 해외로 이전되어 보관 또는 처리 중인 자국민 개인정보에 대하여 일정한 범위에서 외국의 관할권을 제한하기 위한 개념 정의, 논리, 법제화 방안에 대하여도 논의한다. 이런 관점에서 해외로 이전된 자국민 개인정보에 대한 치외법권(extraterritoriality) 개념을 적용한 '데이터 치외법권' 법제의 필요성을 검토하거나 상기 해외 이전된 자국민 개인정보에 대한 외국정부의 관할권을 배제하기 위해 국제법상 '역외 적용 (extraterritorial application)' 용어의 활용 방안도 검토한다. 이상의 연구를 바탕으로 하여 개인정보보호법 등 국내법에의 법제화나 정책 추진 방향을 제시하는 것을 연구의 범위로 삼는다.

## Ⅱ. 연구의 방법

연구방법은 크게 문헌 분석과 전문가 자문으로 수행한다. 문헌 분석의 경우에는 해외 사례 및 국내 논의 동향 등에 관한 문헌 수집 및 분석을 실시하여 비교분석에 활용하고, 전문가 자문의 경우에는 개인정보보호 분야의 전문가 및 국제법 관련 전문가 자문을 통한 연구 결과의 정확성을 담보하고자 한다.

korea
legislation
research
institute

# 제2장
# 자국민의 개인정보보호를 위한 개인정보보호법제 해외 사례 분석

# 제2장 자국민의 개인정보보호를 위한 개인정보보호법제 해외 사례 분석

## 제1절 EU

### Ⅰ. EU 일반개인정보보호규정

#### 1. 개 요

개인정보의 국가간 이동에 대하여 최근 가장 주목을 받고 있는 법제 동향으로서 EU의 일반개인정보보호규정(General Data Protection Regulation; 이하 'GDPR'이라고 한다.)[1]의 제정을 들 수 있다.[2] EU 집행위원회(Commission)에서 입법절차를 진행한지 4년만에 채택되어 2년의 유예기간을 거치고 2018년 5월 25일부터 시행되었다. 이전에 유럽연합 정보보호지침(The Data Protection Directive; 이하 '지침 95/46/EC'라고 한다.)[3]이 EU회원국의 개인정보에 대한 입법지침 역할을 하였지만 2016년 5월 27일 GDPR이 채택된 이후 EU회원국은 GDPR의 직접적인 법적효력을 받게 되었다.[4]

1) EU GDPR의 정식명칭은 "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 (General Data Protection Regulation)"이다.

2) EU GDPR이 제정되기 전까지의 EU의 개인정보 국외이전에 관한 법적 규율에 대한 상세는 최경진, "개인정보 국외이전에 관한 소고", 「법학논총」, 제20집 제1호(2013), 31-63면 참조.

3) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data.

4) EU Official Journal of the European Union issue L119, 2018.5.15

## 2. 제정 배경 및 목적

현대의 정보통신기술(ICT)의 급속한 발달로 인하여 정보를 공유하고 수집하는 규모가 급격히 증가하면서 개인정보에 대한 가치가 높아지게 되었다. 공공기관뿐만 아니라 기업들도 정보를 이용하여 이윤을 추구하게 되면서 개인정보보호의 측면에서도 중요한 변화를 가져오게 되었다. 특히 개인정보의 유통과 관련하여 개인정보보호의 필요성이 대두되면서 이전에 입법지침이었던 지침 95/46/EC으로는 개인정보보호에 한계를 느끼게 되었다. 지침 95/46/EC는 유럽 내에서 개인정보보호방침을 집행하는 데 일관성이 결여되거나, 법적인 불확실성 또는 온라인에서 활동하는 개인을 보호하는데 한계가 있었다. 또한 지침 95/46/EC은 각 회원국이 이를 기준으로 별도의 입법을 제정하고, 그러므로 인하여 각 회원국의 법령 간 규제수준이 다름으로 인하여 국가마다 개인정보보호권 등 개인의 권리와 자유의 보호 수준이 차이를 보였고 이로 인하여 유럽 전체의 자유로운 개인정보의 흐름을 방해할 수 있다는 문제를 내포하고 있었다. 결국 이러한 차이는 유럽연합 차원의 경제활동을 추구하는 데 장애가 되고, 경쟁을 왜곡하고 유럽연합 법률에 따른 기관들이 맡은 임무를 수행하는 데 방해할 수 있다.[5)]

따라서 디지털경제 시장에서 정보의 중요도가 높아짐에 따라 정보보호의 중요성이 강조되게 되면서 EU는 이러한 시장을 통일화하고 법적 불확실성을 해소하기 위하여 보다 강력하고 통일적인 EU 개인정보보호규정을 제정하게 된 것이다. EU 개인정보보호규정은 자연인의 국적 또는 거주지 상관없이 개인의 기본적 권리와 자유로써 존중되어야 함을 기본원칙으로 하고, EU 역내의 개인정보보호에 대한 일관성을 유지하고, 개인을 높은 수준으로 보호하며, 역내 개인정보의 이동에 제약을 제거하여 EU 회원국 간 정보이동을 자유롭게 하고 개인들은 자신들의 개인정보를 통제할 수 있으며, 사업자들과 공적 기관들에게는 법적・실무적 확실성을 실시할 수 있을 것으로 보고 있다.[6)]

---

5) REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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 (General Data Protection Regulation), COD(2012) 11 final, 2016.4.6

6) COD(2012) 11 final, 2016.4.6., p5

## 3. 주요내용

### 1) 적용대상

개인정보는 식별된 또는 식별 가능한 자연인과 관련된 일체의 정보를 가리킨다. 식별 가능한 자연인이란 직·간접적으로 이름, 식별번호, 위치정보, 온라인 식별자를 통하거나 신체적, 심리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성과 같은 특이한 하나 이상의 요인을 통하여 식별이 가능한 자를 가리킨다. 따라서 살아있는 사람을 그 대상으로 하기 때문에 사망한 사람의 개인정보에는 적용되지 않는다.[7] 또한 자연인만 해당되기 때문에 개인이 아닌 법인의 이름, 연락처 등에도 적용되지 않는다.

### 2) 적용범위

GDPR은 실제 개인정보가 EU 역내에서 처리가 이루어지는지 여부에는 관계없이 EU 역내에 컨트롤러 또는 프로세서[8]의 사업장을 운영하고, 개인정보 처리를 수반하는 경우 적용된다. 또한 정보주체가 실제로 재화 또는 서비스의 비용을 지불하였는지 여부와는 관계없이 EU 역외에 컨트롤러 또는 프로세서가 EU 역내에 거주하는 정보주체에게 재화나 서비스를 제공하는 경우 적용된다. 이 때문에 EU 역외의 컨트롤러나 프로세서는 GDPR을 준수하여 야 한다. 이외에도 EU 역내에서 발생하는 정보주체의 행태를 모니터링 하는 경우에 적용된다. 이러한 장소적 적용범위의 확장은 정보주체를 보다 실질적으로 보호하기 위해서이다.

---

7) 각 회원국은 망자의 개인정보 처리에 대한 규정을 정할 수 있다.

8) EU GDPR은 컨트롤러(controller)와 프로세서(processor)라는 용어를 사용하여 GDPR의 수범주체를 정의한다. 컨트롤러란 “단독으로 또는 제3자와 공동으로 개인정보 처리의 목적 및 수단을 결정하는 자연인 또는 법인, 공공기관, 기관, 기타 조직(the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data)”(GDPR 제4조 제7호)을 말하며, 프로세서란 “컨트롤러를 대신하여 개인정보를 처리하는 자연인 또는 법인, 공공기관, 기관 또는 기타 조직(a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller)”(GDPR 제4조 제8호)를 말한다. 컨트롤러라는 개념은 우리법 상으로는 개인정보처리자에 대응되는 개념이고, 프로세서라는 개념은 우리 법상 개인정보처리업무 수탁자 또는 개인정보처리업무의 수임인 등으로 파악할 수 있다. 그러나 원문의 의미를 최대한 살리기 위하여 부득이 이 보고서에서는 컨트롤러나 프로세서라는 한글음 표기를 그대로 사용한다.

### 3) EU 단일 법규정 및 One-Stop Shop

GDPR은 지침 95/46/EC와는 달리 회원국은 별도 이행입법 없이 EU 전역에서 단일 법규정으로 적용된다. GDPR의 적용에 대한 모니터링을 전담하기 위해 각 회원국은 개인정보 관련 민원을 접수 및 처리하고 행정 제재를 과하기 위한 하나 이상의 독립된 감독기관(Supervisory Authority)를 설치하게 되며, 각 회원국의 감독기관은 다른 감독기관과 상호 지원 및 공동 활동을 수행하면서 협력하게 된다. 사업자가 EU 역내에 여러 사무소를 두는 경우에 주된 사업장이 소재하는 지역의 주 감독기관(lead supervisory authority)의 단일한 감독을 받게 되어 규제기관 측면에서의 중복을 피하고자 하여 혼란을 덜고자 하였다. 주 감독기관은 해당 사업자의 EU 전역에서의 개인정보의 처리를 감독하는 소위 원스톱샵(one-stop shop)의 기능을 수행한다. 기존의 제29조 작업반(Article 29 Working Party)을 대체하는 유럽정보보호위원회(European Data Protection Board (EDPB), GDPR 제68조)가 각 감독기관을 조정하는 역할을 수행한다.

### 4) 책임성 강화

GDPR는 일정한 기준에 해당하는 컨트롤러나 프로세서에게 GDPR의 각 규정의 준수를 위하여 일정한 의무가 부과된다. 개인정보의 처리가 본 규정에 따라 이루어졌음을 보장하고 입증할 수 있도록 적절한 기술 및 관리조치를 취해야함은 기본이고, 정보보호를 위하여 기획 단계에서부터 기본적으로 정보보호가 높은 수준으로 설정될 수 있도록 정보보호활동을 수행하여야 하고(privacy by design and by default, GDPR 제25조), 그 처리활동의 기록을 보존할 의무(GDPR 제30조)나 개인정보보호 영향평가(GDPR 제35조)를 받을 의무가 있으며, 개인정보보호 담당관(Data Protection Officer)을 지정해야 한다(GDPR 제37조부터 제39조). 개인정보보호 담당관은 직무상의 자질 특히, 개인정보보호법과 실무에 대한 전문적 지식을 갖춰야 하며, 그 구체적인 내용은 개인정보보호 담당관이 책임지게 되는 개인정보 처리 활동에 따라 달라진다. 개인정보보호 담당관은 컨트롤러 또는 프로세서에게 고용되어 활동을 할 수 있지만 서비스 계약 하에서 관련 업무를 수행할 수도 있다. 또한 하나의 기업 그룹은 단일 개인정보보호 담당관을 임명할 수도 있다.

### 5) 프로세서에 대한 규율[9)]

GDPR을 통해 프로세서에게도 직접적인 의무가 부과된다. 그 의무에는 컨트롤러를 위하여 실행되는 정보처리활동의 서면 기록 유지 의무, 개인정보 처리 이전에 해당 법률요건을 컨트롤러에게 고지하여야 할 의무, 적절한 법정 기밀유지의 의무, 개인정보침해가 발행한 경우에 부당한 지연 없이 해당 사실을 컨트롤러에게 통지할 의무, 일정한 경우에 개인정보보호 담당관을 지정할 의무, 일정한 경우에 EU에 법인을 설립하지 않은 자가 대표자를 임명할 의무 등이다. 개인정보 역외이전 규정은 프로세서에게도 적용되며, 프로세서를 위한 의무적 기업규칙(Binding Corporate Rules)도 공식적으로 인정된다.

### 6) 동의요건의 강화

개인정보 보호수준의 강화의 주요 수단 중의 하나인 동의도 강화되었다. GDPR에 따른 유효한 동의 요건은 정보주체와 관련된 개인정보 처리에 대하여 동의한다는 개인정보주체의 바람을 진술 혹은 분명하고 긍정적인 행위를 통해 자유롭게 특정되고, 구체적이며 잘 이해하고, 뜻이 분명하게 나타내는 것을 말한다.(GDPR 제4조) 또한 기타 사안에 관한 서면으로 제공되는 경우에는 알아듣기 쉽고 보거나 이해하는데 분명한 언어를 사용하여 이해하기 쉽고 접근하기 쉬운 형태로서 다른 기타 사안으로부터 분명하게 구별할 수 있는 방식으로 제시되어야 한다. (GDPR 제7조). 컨트롤러는 동의를 받았다는 사실을 증명할 수 있어야 하고, 해당 동의는 철회될 수 있다. 16세 미만의 아동의 경우에는 아동의 부모나 보호자의 동의를 받아야 하며, 입증할 수 있어야 한다(GDPR 제8조). 다만, GDPR은 회원국이 이러한 부모나 보호자의 동의를 요하는 아동의 연령을 16세에서 13세까지 낮출 수 있도록 허용함으로써 EU 전역의 법규범의 조화를 깰 가능성을 내포하고 있다.

9) 최경진, "글로벌 개인정보보호법제 - EU GDPR, 미국 및 일본의 주요 입법 사례를 중심으로," 2017 인터넷정책아카데미 2기 "데이터가 결정하는 미래 - DT 강국으로 가기 위한 입법 방향 - (2017.8.2.) 자료집, 한국인터넷기업협회; 대외경제정책연구원, EU 개인정보보호법(GDPR) 발효: 평가와 대응방안, KIEP 오늘의 세계경제 Vol 18 No. 19, 2018.5.15. 참조.

### 7) 개인정보 침해 통지 의무

컨트롤러는 개인정보침해가 발생한 경우 그 사실을 정보보호감독기관에게 통지하여야 한다. 이러한 통지는 부당한 지체 없이 이루어져야 하며, 가능한 한 해당 사실을 인지한 때로부터 72시간 이내에 이루어져야 한다(GDPR 제33조). 또한 개인정보침해가 자연인의 권리와 자유에 높은 위험을 야기할 수 있는 경우에 컨트롤러는 부당한 지체 없이 개인정보 침해로부터 영향을 받는 정보주체에게도 해당 침해 사실을 알려야 한다(GDPR 제34조).

### 8) 제재

GDPR은 각 감독기관이 최대 전세계 연간 매출액의 4% 또는 2천만 유로 이하의 범위 내에서 더 높은 금액을 위반에 대한 과징금으로 부과할 수 있도록 규정하고 있다. 이에 대한 조문에는 제5조, 제6조, 제7조 및 제9조에 따른 동의 조건을 비롯한 정보처리의 기본 원칙, 제12조-제22조에 따른 개인정보주체의 권리, 제44조-제49조에 따른 제3국이나 국제기구의 수령인에게로의 개인정보 이전, 제9장에 따라 채택된 회원국 법률에 따른 의무, 제58조(2)에 따라 감독기관이 내린 명령, 또는 정보처리의 한시적 또는 확정적 제한, 또는 개인정보 이동의 중지를 준수하지 않거나 열람의 기회를 제공하지 않아 제58조(1)를 위반, 감독기관의 명령 불복이 있다.(GDPR 제83조제5항). 한편, GDPR 제8조, 제11조, 제25조부터 제39조, 제42조와 제43조에 따른 컨트롤러나 프로세서의 의무 위반과 같은 경우 또는 제42조 및 제43조에 따른 인증 기관의 의무, 제41조(4)에 따른 모니터링 기관의 의무 위반 시에는 전세계 연간 매출액의 2% 또는 1천만 유로 이하의 범위 내에서 더 높은 금액을 과징금으로 부과할 수 있다(제83조제4항).

### 9) 정보주체의 권리

정보주체의 권리 중에서 가장 주목받았던 것은 GDPR 초안으로부터 촉발된 소위 잊혀질 권리(right to be forgotten)이다. 잊혀질 권리는 구글 스페인 사건에 관한 유럽사법재판소(European Court of Justice) 판결(Google Spain SL, Google Inc. v Agencia Española de

Protección de Datos, Mario Costeja González)을 통해서 다시 한 번 주목받은 이후 최종 GDPR에서는 삭제권(잊혀질 권리, right to be forgotten)으로 규정되었다(GDPR 제17조). 이에 따르면 잊혀질 권리란 정보주체가 개인 정보 처리에 대한 동의를 철회하고 더 이상 합법적인 처리근거가 없는 경우와 같은 일정 상황 하에서 정보주체가 컨트롤러에서 부당한 지체 없이 해당 정보를 삭제할 것을 요구할 수 있도록 권리로서 인정한 것이다. 이외에 GDPR은 개인정보를 다른 컨트롤러에게 쉽게 이전할 수 있는 형태로 개인정보를 반환받을 수 있는 권리를 인정함으로써 소위 '정보 이동성(data portability)'을 보장하고 있다(GDPR 제20조).

### 10) 개인정보의 역외이전

GDPR 제5장(제44조부터 제49조)는 국경간 개인정보의 이전을 규율하고 있다. 제45조는 국외 이전 허용 근거로서 적절성 결정(adequacy decision)[10]을 규정한다. 제46조는 적절성 결정이 없는 경우 적절한 세이프가드(appropriate safeguards)에 의한 이전의 요건을 규정한다. 제47조는 구속력 있는 기업규칙(binding corporate rules)을 규정하고, 제48조는 외국 법원이나 행정청이 GDPR에 의하여 허용되지 않는 이전을 명령하는 상황을 규율한다. 제49조는 적절성 결정이나 적절한 세이프가드가 없는 경우의 특정 상황에서의 수정조건을 규정한다. 자세한 내용은 아래에서 다루도록 하겠다.

**<표 2-1> EU GDPR의 주요내용**

| GDPR 체계 | |
|---|---|
| 일반규정 (제1장) | 목적(1), 물적 범위(2), 장소적 범위(3), 정의(4) |

10) EU GDPR 상의 "adequacy decision"의 번역을 기존에 적정성 결정으로 사용하는 경우가 많았다. 그런데 GDPR 상의 adequate이나 adequacy는 정도나 기준에 꼭 알맞은 것을 의미하는 '적절하다'는 의미로 파악하는 것이 더욱 정확해 보인다. 이러한 의미에 따라 이 보고서에서는 '적절성 결정'이라는 단어로 사용한다. 최경진, 전게 "개인정보 국외이전에 관한 소고", 37-40면 참조.

| | | |
|---|---|---|
| 원칙<br>(제2장) | 개인정보 처리 관련 원칙(5), 처리의 적법성(6), 동의조건(7), 정보사회서비스에 관한 아동의 동의에 적용되는 조건(8), 특정범주의 개인정보 처리(9), 범죄경력 및 범죄행위에 관한 개인정보의 처리(10), 식별을 요하지 않는 처리(11) | |
| 정보주체 권리<br>(제3장) | 제1절 투명성 및 형식 | 정보주체의 권리를 행사하기 위한 투명한 정보, 통신 및 형식(12) |
| | 제2절 정보 및 개인정보 접근 | 정보주체로부터 개인정보를 수집하는 경우 제공되는 정보(13), 정보주체로부터 개인정보가 수집되지 않는 경우 제공되는 정보(14), 정보주체의 접근권(15) |
| | 제3절 정정 및 삭제 | 정정권(16), 삭제권(잊혀질 권리)(17), 처리에 대한 제한권(18), 개인정보의 정정이나 삭제 또는 처리제한에 관한 고지의무(19), 정보이동권(20) |
| | 제4절 반대할 권리 및 자동적인 개별의사결정 | 반대할 권리(21), 프로파일링을 포함하는 자동적인 개인의사결정(22) |
| | 제5절 제한 | 제한(23) |
| 컨트롤러와 프로세서<br>(제4장) | 제1절 일반적인 의무 | 컨트롤러의 책임(24), 설계에 의한 그리고 기본으로서의 정보보호(25), 공동 컨트롤러(26), 유럽연합 내에 설립되지 않은 컨트롤러 또는 프로세서의 대리인(27), 프로세서(28), 컨트롤러 또는 프로세서의 권한에 따른 처리(29), 처리 활동의 기록(30), 감독기관과의 협력(31) |
| | 제2절 개인정보의 보안 | 처리의 보안(32), 감독기관에 대한 개인정보 침해 통지(33), 정보주체에 대한 개인정보 침해 통지(34) |
| | 제3절 정보보호 영향평가 및 사전자문 | 정보보호 영향평가(35), 사전자문(36) |
| | 제4절 정보보호 담당관 | 정보보호 담당관의 지정(37), 개인정보보호 담당관의 지위(38),<br>개인정보보호 담당관의 임무(39) |
| | 제5절 행동강령 및 인증 | 행동강령(40), 승인된 행동강령의 모니터링(41), 인증(42), 인증기구(43) |

| | | |
|---|---|---|
| 제3국 또는 국제기구로의 개인정보 이전 (제5장) | 이전을 위한 일반원칙(44), 적절성 결정에 기초한 이전(45), 적절한 안전조치에 의한 이전(46), 구속력 있는 기업규칙(47), 유럽연합 법률로 허가되지 않은 이전 또는 공개(48), 특정 상황을 고려한 적용제외(49), 개인정보 보호를 위한 국제협력(50) | |
| 독립 감독 기구 (제6장) | 제1절 독립적인 지위 | 감독기관(51), 독립성(52), 감독기관 위원의 일반 요건(53), 감독기관 설치에 관한 규칙(54조) |
| | 제2절 기능, 임무 및 권한 | 기능(55), 주 감독기관의 기능(56), 임무(57), 권한(58), 활동 보고서(59) |
| 협력 및 일관성 (제7장) | 제1절 협력 | 주 감독기관와 관련된 다른 감독기관 간 협력(60), 상호지원(61), 감독기관의 공동활동(62) |
| | 제2절 일관성 | 일관성 메커니즘(63), 유럽정보보호이사회 의견(64), 유럽정보보호이사회에 의한 분쟁해결(65), 긴급 절차(66), 정보의 교환(67) |
| | 제3절 유럽정보보호이사회 | 유럽정보보호이사회(68), 독립성(69), 유럽정보보호이사회의 임무(70), 보고서(71), 절차(72), 의장(73), 의장의 임무(74), 사무국(75), 비밀(76) |
| 구제, 책임 및 처벌 (제8장) | 감독기관에 민원을 제기할 권리(77), 감독기관를 상대로 한 효과적인 사법구제권(78), 컨트롤러나 프로세서를 상대로 한 효과적인 사법구제권(79), 정보주체의 대리(80), 법적 절차의 중지(81), 보상에 대한 권리 및 책임(82), 행정 과태료 부과에 관한 일반조건(83), 처벌(84) | |
| 특정 처리 상황에 관한 규정 (제9장) | 처리 및 표현과 정보의 자유(85), 처리 및 공식 문서에 대한 일반인의 접근(86), 국가 식별번호의 처리(87), 고용 맥락에서의 처리(88), 공익을 위한 기록보존 목적, 과학이나 역사연구 목적 또는 통계 목적을 위한 처리와 관련한 안전조치 및 적용 제외(89), 비밀유지 의무(90), 교회 및 종교단체의 현행 정보보호 규정(91) | |
| 위임법률 및 시행법률 (제10장) | 위임의 행사(92), 위원회의 절차(93) | |
| 최종규정 (제11장) | 지침95/46/EC의 폐지(94), 지침2002/58/EC와의 관계(95), 이전에 체결된 협정과의 관계(96), 집행위원회 보고서(97), 기타 유럽연합의 정보보호 법률에 대한 검토(98), 발효 및 적용(99) | |

출처: 최경진, EU GDPR의 분석 및 시사점, Naver Privacy White Paper

## Ⅱ. EU GDPR 상의 역외적용 및 역외이전 규율체계 분석[11)]

### 1. 총칙

GDPR은 현재 처리 중이거나 제3국 또는 국제기구로의 이전 후에 처리될 예정인 개인정보는 해당 제3국이나 국제기구로부터 기타 제3국이나 국제기구로 개인정보가 이전되는 경우 등 조문에 따라 컨트롤러와 프로세서가 규정된 조건을 준수하는 경우에만 그 이전을 가능하게 하고 있다. 이는 규정을 통해 보증되는 개인의 보호 수준을 보장하기 위해 적용되어야 함을 강조하고 있다.[12)]

제46조 하에서 인정되는 적절한 세이프가드의 예로서는 (1) 공공기관 간의 법적으로 구속력 있고 집행가능한 법률문서, (2) 제47조에 따른 구속력 있는 기업규칙, (3) 집행위원회가 채택한 표준 정보보호 조항, (4) 감독기관가 채택하고 집행위원회가 승인한 표준 정보보호 조항, (5) 제3국에서 적절한 세이프가드를 적용하는 컨트롤러나 프로세서의 구속력 있고 집행가능한 약정과 함께 제40조에 따른 승인된 행동강령, (6) 제3국에서 적절한 세이프가드를 적용하는 컨트롤러나 프로세서의 구속력 있고 집행가능한 약정과 함께 제42조에 따른 승인된 인증 체계(approved certification mechanism)가 있다. 이러한 인증의 예로서 유럽정보보호인장(European Data Protection Seal)이 인정된다.

### 2. EU GDPR 상의 역외이전 요건

#### 1) EU 개인정보보호 적절성 결정에 따른 이전

##### ① 총칙

제3국 또는 국제기구로의 개인정보 이전은 집행위원회가 제3국, 해당 제3국의 영토나 하나 이상의 지정 부문, 또는 국제기구가 적절한 보호수준을 보장한다고 결정한 경우 가

11) COD(2012) 11 final, 2016.4.6., p185-198
12) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 Article 44

능하도록 하고 있다.

### ② 적절성 평가의 고려 사항

집행위원회의 개인정보보호 수준의 적절성을 평가하는 사항에는 법치주의, 인권 및 기본적 자유의 존중, 공공 보안, 방위, 국가 안보 및 형사법 및 개인 정보에 대한 공공 기관의 접근에 관한 일반 및 부문별 관련 법안, 해당 국가 또는 국제기구에서 준수하는 제3국 또는 국제기구에 개인정보를 이전하는 규칙을 포함하여 정보보호 규칙, 사법적 판례, 개인정보가 전송되는 정보주체에 대한 효과적이고 시행 가능한 정보주체 권리 및 효과적인 행정 및 사법적 구제책이다. 또한 적절한 제재 권한을 포함하여 데이터 보호 규칙의 준수를 보장하고 집행할 책임이 있는 제3국 또는 국제기구가 소속된 하나 이상의 독립된 감독기관의 존재와 효과적인 기능, 적절한 시행 권한을 포함한 정보보호 규칙의 준수를 보장하고 집행하며 정보주체가 자신의 권리를 행사하는 데 도움을 주고 조언하며 회원국의 감독기관과 협력할 책임과 관련 제3국 또는 국제기구의 국제 공약, 특히 개인 정보의 보호와 관련하여 법적으로 구속력이 있는 협약이나 수단뿐만 아니라 다국간 또는 지역 시스템에의 참여로 인해 야기된 기타 의무도 있다.

### ③ 사후 규제

이러한 평가는 최소 4년마다 제3국이나 국제기구 내의 관련 추가사항을 포함하여 정기적으로 검토해야 한다. 그리고 집행위원회는 이러한 적절성 결정의 결과를 유럽연합 관보 및 웹사이트에 게재하도록 한다. 이후에도 지속적인 모니터링을 통하여 적절한 보호 수준이 보장되지 않는다고 판단될 경우, 먼저 제3국과 국제기구와 협의를 통해 이를 시정하도록 하고 충분히 타당하고 긴요한 시급성의 근거가 있는 경우에는 필요한 정도까지 소급효 없이 개인정보 이전결정을 철회, 수정, 또는 중지시킬 수 있다.

### 2) 개인정보보호 적절성 평가에 의거한 결정이 없는 경우

#### ① 표준 개인정보보호 조항(Standard data protection clauses)에 의한 이전

GDPR은 집행위원회의 적절성 평가에 의한 결정이 없는 경우, 컨트롤러 또는 프로세서는 적절한 안전조치를 제공하여 시행 가능한 정보주체 권리 및 정보주체에 대한 효과적인 법적 구제가 가능하다는 조건하에 개인정보를 제3국 또는 국제기구로 이전 할 수 있도록 하고 있다. 제93조 제2항에 따른 심사 절차에 따라 위원회가 채택한 표준 개인정보보호 조항, 감독기관이 채택하고 집행위원회가 제93조 제2항에 따른 심사 절차에 따라 승인한 표준정보보호 조항을 통해 개인정보 이전을 가능하게 하고 있다.

#### ② 의무적 기업규칙(Binding corporate rules)

GDPR은 적절한 안전조치 중 하나로 감독기관의 특별한 승인을 요하지 않고 개인정보를 이전할 수 있는 경우 중의 하나로 의무적 기업규칙을 두고 있다. GDPR의 의무적 기업규칙은 기존에 있던 의무적 기업규칙(BCRs)의 요건을 법제화한 것이다. 의무적 기업규칙은 GDPR 제63조에 따라 일관적인 매커니즘을 보여야 하고 아래의 경우를 전제로 승인을 받아 개인정보를 이전할 수 있다. 의무적 기업 규칙에 대해 컨트롤러, 프로세서, 감독기관 사이에 이루어지는 정보 교환에 필요한 양식과 절차를 정할 수 있다.

<표 2-2> 의무적 기업규칙의 전제 및 명시 요건[13)]

| | |
|---|---|
| 전제 | 법적 구속력이 있으며 피고용인 등 공동 경제활동에 관여하는 사업체 집단 또는 기업집단의 모든 구성원들에게 적용되고 그들에 의해 이행되는 경우 |
| | 본인의 개인정보 처리와 관련하여 개인정보주체에게 명시적으로 구속력 있는 권리를 부여하는 경우 |
| | 제47조 제2항의 요건을 충족시키는 경우 |

13) GDPR 제47조. GDPR 전체 번역본 및 추가 관련 자료에 대하여는 개인정보보호위원회 “GDPR 자료실” 참조.

| | |
|---|---|
| 명시 요건 | 사업체 그룹의 구조 및 연락 세부 사항 또는 공동 경제 활동과 각 회원국의 기업 집단 |
| | 개인 정보의 범주, 처리 유형 및 목적, 영향을 받는 데이터 유형 및 문제의 제3국 또는 국가의 식별을 포함한 데이터 전송 또는 전송 집합 |
| | 내부적으로나 외부적으로 그들의 법적 구속력이 있는 성질 |
| | 제한된 저장 기간, 디자인 및 기본적으로 데이터 보호, 처리, 개인 데이터의 특수 범주의 처리, 데이터 보안을 보장하기 위한 조치에 대한 법적 근거에 대한 일반적인 데이터 보호 원칙의 응용, 특히 목적 제한; 그리고 의무적 기업 규칙에 구속되지 않는 단체로의 전진에 관한 요구 사항 |
| | 처리와 관련한 데이터 주체의 권리 및 그러한 권리를 행사할 수 있는 권리 (제 22조에 따라 프로파일링을 포함하여 자동 처리에만 근거한 결정의 대상이 되지 아니하는 권리를 포함한다), 권한 있는 감독관에게 민원을 제기 할 권리 제79조에 따라 회원국의 관할 법원에 제소하고, 의무적 기업 규칙 위반에 대한 배상 및 보상 |
| | 해당 회원국이 설립하지 않은 관련 단체의 의무적 기업 규칙 위반에 대해 회원국 영토 내에서 설립 된 관리자 또는 프로세서의 수락; 컨트롤러 또는 프로세서는 그 회원이 손해를 초래하는 사건에 대해 책임이 없다는 것을 입증하는 경우에만 그 책임의 전부 또는 일부 면제 |
| | 제13조 및 제14조에 더하여, 본 단락의 (d), (e) 및 (f) 항에 명시 된 규정에 대한 제반 회사 규칙에 관한 정보가 개인정보주체에게 제공되는 방식 |
| | 제 37 조에 따라 지정된 데이터 보호 책임자 또는 해당 기업 그룹 내의 의무적 기업 규칙 또는 공동 경제 활동에 종사하는 기업 그룹의 준수를 감시하는 책임을 맡은 다른 사람 또는 주체의 업무뿐만 아니라 모니터링 교육 및 민원 처리 |
| | 민원 처리 절차 |
| | 기업 집단 내에서의 메커니즘, 또는 의무적 기업규칙 준수 확인을 위한 공동 경제 활동에 종사하는 기업 그룹. 이러한 메커니즘은 데이터 보호 감사 및 데이터 주체의 권리를 보호하기 위한 시정 조치를 보장하는 방법을 포함해야한다. 그러한 검증의 결과는 요점 (h)에 언급 된 사람 또는 단체 및 사업체 그룹 또는 공동 경제 활동에 종사하는 기업 집단의 지배 사업 책임자에게 전달되어야하며, 권한있는 감독 기관에 요청 |
| | 규칙의 변경을 보고하고 기록하고 그 변경 사항을 감독 기관에 보고하는 메커니즘 |

#### ③ 승인된 행동강령(approved code of condust) 또는 승인된 인증제도(approved certification)

정보주체의 권리와 관련하여 적절한 보호책을 적용하기 위해 제3국의 컨트롤러 또는 프로세서의 구속력이 있고 집행 가능한 약속을 포함한 제40조에 따라 공인된 행동 강령 또는 정보주체의 권리를 포함하여 적절한 안전장치를 적용하기 위해 제3국의 컨트롤러 또는 프로세서의 구속력 및 집행 약속을 포함한 제42조에 의해 공인된 인증 메커니즘이 있다.

### 3. 특정 사항에 대한 적용의 일부 제외

특정 사항에 대한 적용의 일부 제외로 GDPR은 예외적으로 개인정보 이전에 관한 예외적인 규정을 두고 있다.[14] 그 구체적인 사항으로는 적절성 결정 및 적절한 안전조치가 없음으로 인해 그 같은 개인정보의 이전이 개인정보주체에 초래할 수 있는 위험을 고지받은 후 개인정보주체가 명시적으로 이전에 동의한 경우,[15] 개인정보주체와 컨트롤러 간의 계약을 이행하기 위해서나 개인정보주체의 요청으로 취한 계약 사전 조치를 이행하는데 이전이 필요한 경우,[16] 개인정보주체의 이익을 위해 컨트롤러와 기타 자연인 또는 법인 간에 체결된 계약의 이행을 위해 이전이 필요한 경우,[17] 중요한 공익상의 이유로 정보이전이 필요한 경우,[18] 법적 권리의 확립, 행사, 방어를 위해 정보이전이 필요한 경우,[19] 개인정보주체가 물리적 또는 법률적으로 동의를 할 수 없는 경우로서 개인정보주체 또는 타인의 생명과 관련한 주요 이익을 보호하기 위해 정보이전이 필요한 경우,[20] 개인정보가 유럽연합 또는 회원국 법률에 따라 정보를 공개할 목적이거나 일반 국민 또는 정당한 이익을 입증할 수 있는 제3자가 참조(조회)하기 위한 목적으로 만들어진 개인정보 등록부

14) GDPR 제49조.
15) GDPR 제49조 제1항 (a).
16) GDPR 제49조 제1항 (b).
17) GDPR 제49조 제1항 (c).
18) GDPR 제49조 제1항 (d).
19) GDPR 제49조 제1항 (e).
20) GDPR 제49조 제1항 (f).

(register)로부터 유럽연합 또는 회원국 법률에 명시된 참조(조회)의 조건이 충족되는 범위 내에서 이전되는 경우[21]가 있다.

이 예외적인 사항은 정보의 이전이 의무적 기업 규칙에 대한 규정 등 제45조나 제46조의 규정을 근거로 할 수 없고, 위 경우에 따른 특정 상황에서의 일부 제외가 적용되지 않는 경우에는 정보이전이 반복적이지 않고, 한정된 숫자의 정보주체에만 적용되고 개인정보주체의 이익이나 권리 및 자유가 우선하지 않는 한 개인정보처리자의 정당한 이익의 목적에 필요하며, 컨트롤러가 정보이전과 관련한 일체의 정황을 평가한 후 그 결과를 토대로 개인정보 보호에 적절한 안전조치를 제시하는 경우에만 제3국이나 국제기구로의 개인정보이전이 가능하다. 컨트롤러는 정보이전 사실을 감독기관에 고지해야 한다. 제13조 및 제14조에 명시된 정보 제공 이외에도 컨트롤러는 해당 이전 및 본인의 설득력 있는 정당한 이익에 관한 정보를 정보주체에 고지해야 한다.

## 제2절 일 본

### Ⅰ. 개인정보의 보호에 관한 법률

#### 1. 개 요

일본도 최근 정보통신기술의 발달로 인하여 개인정보 보호에 관한 법률 재정당시에는 상용되지 않았던 개인정보의 이용가치가 점점 더 높아지게 되면서 이전에 시행되고 있던 개인정보보호법으로는 개인정보에 관한 사항의 범위와 규칙이 불분명해지게 되어 개인정보의 활용환경에 대한 정비를 위하여 2017년 5월 30일 이후 「개인정보의 보호에 관한 법률(個人情報の保護に關する法律)」(이하 "일본 개정개인정보보호법"이라 한다)을 개정하여 개인정보의 국외이전에 관한 규율체계를 재정립하였다.[22]

21) GDPR 제49조 제1항 (g).

22) 허중혁, "일본 개인정보보호법 개정안 5월30일 전면시행", 법률신문 해외소식(2017.3.22.자), <https://www.lawtimes.co.kr/Legal-News/Legal-News-View?serial=108889> (2018.10.31. 최종방문)

## 2. 개정 배경 및 목적

일본 개정개인정보보호법은 고도의 정보통신사회의 발달에 따라 개인 정보의 이용이 크게 확대되고 있는 점을 감안하여 개인 정보의 적정한 취급에 관한 기본 이념 및 정부의 기본 방침의 작성 기타 개인 정보 보호에 관한 시책의 기본이 되는 사항을 정하고, 국가 및 지방 공공 단체의 책무 등을 분명히 함과 동시에 개인 정보를 취급하는 사업자의 준수해야 할 의무 등을 규정함으로써 개인 정보의 적절하고 효과적인 활용이 새로운 산업의 창출 및 활력있는 경제 사회와 풍요로운 국민 생활의 실현에 이바지 것임을 기타 개인 정보의 유용성에 배려하면서 개인의 권리 이익을 보호하는 것을 목적으로 한다.[23]

## 3. 주요내용

### 1) 개인정보의 정의 명확화

개정전의 개인정보보호법에서는 보호대상으로서, 생존하는 개인에 관한 정보 중 특정의 개인을 식별할 수 있는 것과 다른 정보와 용이하게 조합할 수 있고 그것에 의해 특정의 개인을 식별할 수 있는 것을 「개인정보」로 하고 있었다.[24] 예를 들어 기상데이터는 개인정보보호법에 적용이 되지 않는다. 그런데 정부나 기업에서 수집하고 사용하게 되는 데이터는 기상데이터 등 극소수의 데이터를 제외하면 대부분 개인정보이거나 개인정보가 될 가능성이 있는 정보여서 개인정보법제의 잠재적 적용대상이 되기 때문에 이에 대하여 명확화를 할 필요가 있었다.[25] 개정 이후 개인정보에 대한 정의를 명확화하여 개인정보는 살아있는 개인에 관한 정보를 말한다는 것은 같으나 여기에 포함되어있는 것은 성명, 생년월일 기타 기술[26] 등에 기재된 혹은 기록되거나 음성 작동 다른 방법을 사용하여 표현 된 일체의 사항에 의해 특정 개인을 식별할 수 있는 것[27]을 말한다.

---

23) 일본 개인정보보호법 제1조.
24) 한귀현 (2017). 일본 개정개인정보보호법의 주요내용과 그 시사점. 공법학연구, 18(4), 535면
25) 경성대학교 산학협력단, 일본의 개인정보보호 법제・정책 분석에 관한 연구, 개인정보보호위원회, 2017.12., 17면.
26) 문서, 도화 또는 전자적 기록에서 만들어지는 기록을 말한다. 일본 개정개인정보보호법 제18조제2항에서 같다
27) 다른 정보와 용이하게 조합 할 수 있으며, 그로 인하여 특정 개인을 식별 할 수 있는 것을 포함한다.

### 2) 익명가공정보

익명가공정보란 특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻는 개인에 관한 정보로서, 해당 개인정보를 복원할 수 없도록 한 것을 의미한다. 익명가공정보의 핵심은 해당 정보를 통해 개인을 식별할 수 없도록 하는 것은 물론 이를 복원하여 특정 개인을 재식별 할 수 없도록 하는 것을 포함한다. 비식별 가공 및 재식별 방지 조치는 개인정보 취급 사업자 또는 익명가공정보 취급사업자가 통상적인 방법[28]을 통해 해당 정보에서 개인을 특정할 수 없도록 하는 것을 의미한다. 통계정보는 특정 개인과 매칭되어 식별되지 않는 한, 법에서 정하는 '개인에 관한 정보'에 해당하지 않으므로, 개정 이전 법에서 규정된 바와 같이 규제 대상에서 제외한다.

일본의 익명가공정보라고 하여도 데이터를 가공해 주는 자가 원본데이터를 폐기하지 않은 이상 식별가능성이 잔존할 수 있으나 이를 개정법에 금지하여 익명성을 보장하고 있는 것이 일본 익명가공정보의 특징이다.[29]

**<표 2-3> 일본 개인정보에 관한 법률체계**

| 일본 개인정보에 관한 법률 체계 | |
|---|---|
| 제1장 총칙 | 목적(1), 정의(2) |
| 제2장 국가 및 지방 공공 단체의 책무 등 | 기본이념(3), 국가책무(4), 지방 공공 단체의 책무(5), 법제상의 조치 등(6) |
| 제3장 개인 정보의 보호에 관한 시책 등 | 개인 정보 보호에 관한 기본 방침(7) |
| | 지방 공공 단체 등의 지원(8), 고충 처리를 위한 조치(9), 개인 정보의 적정한 취급을 확보하기위한 조치(10) |
| | 지방 공공 단체 등이 보유하는 개인 정보의 보호(11) 지역 내의 사업자 등에 대한 지원(12)민원처리 등(13) |
| | 국가 및 지방 공공 단체의 협력(14) |

28) 일반인 및 일반 사업자의 능력과 기술 등을 기준으로 한다.
29) 경성대학교 산학협력단, 일본의 개인정보보호 법제 · 정책 분석에 관한 연구, 개인정보보호위원회, 2017.12., 17면.

| | |
|---|---|
| 제4장 개인 정보 취급 사업자의 의무 등 | 이용 목적의 특정 (15), 이용 목적에 의한 제한(16), 적정한 취득(17), 취득시의 이용 목적의 통지 등(18), 데이터 내용의 정확성 확보 등(19), 안전 관리 조치(20), 종업원의 감독(21), 위탁처의 감독(22), 제삼자 제공의 제한(23), 외국의 제삼자에게의 제공의 제한(24), 제삼자 제공에 관한 기록의 작성 등(25), 제삼자 제공을 받을 때 확인 등(26), 보유 개인 데이터에 관한 사항의 공표 등(27), 공개(28), 정정 등(29), 이용 정지 등(30), 이유 설명(31), 공개 등의 청구 등에 응하는 절차(32), 수수료(33), 사전 신청(34), 개인 정보 취급 사업자에 의한 불만 처리(35) |
| | 익명 가공 정보의 작성 등(36), 익명 가공 정보의 제공(37), 식별 행위의 금지(38), 안전 관리 조치 등(39) |
| | 보고 및 현장 검사(40) |
| | 제4절 민간 단체에 의한 개인 정보 보호의 추진 (47-58) |
| 제5장 개인 정보 보호위원회 (59-74) | |
| 제6장 그 외 규칙 (75-81) | |
| 제7장 벌칙 (82-88) | |

일본의 구법에서는 개인정보의 역외 이전에 관한 특별 규정이 없었으나 개정개인정보보호법에서는 제23조에 제3자 제공의 제한이라는 규정을 신설하여 제3자의 개인정보에 대한 접근을 제한하고 있다.

## Ⅱ. 일본 개인정보 역외이전에 대한 규율체계

개정 개인정보보호법 제75조는 '국내에 있는 자에 대한 물품 또는 역무의 제공에 관련하여 그 자를 본인으로 하는 개인정보를 취득한 개인정보취급사업자가 외국에서 당해 개인정보 또는 당해 개인정보를 사용하여 작성한 익명가공정보를 취급하는 경우에 관해서도 적용한다.'라고 규정하여 이른바 역외적용의 규정을 새로이 두고 있다. 이전의 개인정보보호법은 속지주의의 사고 등으로 인하여 외국의 사업자에 의한 개인정보의 취급에는 적용되지 않는 것으로 이해되었다.[30] 그러나 기업활동의 글로벌화나 전자상거래의 보

30) 한귀현 (2017). 일본 개정개인정보보호법의 주요내용과 그 시사점. 공법학연구, 18(4), 545면.

급 등에 수반하여 외국에서 직접 일본에 향하여 인터넷 등으로 물품의 판매나 서비스를 제공하고, 일본의 거주자 등으로부터 개인정보를 취득하는 사업자가 점증함에 따라, 이와 같은 사업자에 있어서도 개인정보의 적정한 취급을 확보할 필요성이 대두됨에 따라 역외 적용의 규정이 두어진 것이다. 다만, 개정된 제75조는 개인정보보호법의 모든 규정을 적용하는 것이 아니라 외국 사업자라고 하더라도 일본의 거주자 등으로부터의 개인정보의 취득은 그 중요한 부분이 일본 역내에서 행해지고 있기 때문에 속지주의에 근거하여 특별한 규정이 없다고 하더라도 일본법이 적용된다고 보아 개인정보보호법 제17조(적정한 취득)과 제18조제2항(취득시의 이용목적의 명시)은 열거하고 있지 않다. 또한 법의 역외 적용이 입법관할권과의 관계에서 허용되었다 하더라도 외국에서 일본의 행정기관이 법을 집행할 수 있는지 여부라는 집행관할권의 문제로 인하여 개정개인정보보호법 제75조는 보고 및 출입검사(동법 제40조), 명령(동법 제42조 제2항・제3항)의 규정은 역외적용의 대상으로는 하고 있지 않다.[31]

제75조 외에도 제24조(외국에 있는 제3자에의 제공제한)를 신설하여 개인정보의 역외 이전에 대하여 제한하고 있다. 개인 정보 취급 사업자는 외국[32]에 있는 제3자[33]에게 개인 정보를 제공하는 경우에는 법령에 근거하는 경우, 사람의 생명, 신체 또는 재산의 보호를 위하여 필요한 경우로서 본인의 동의를 얻기 어려운 경우, 공중 위생의 향상 또는 아동의 건전한 육성 추진을 위해 특히 필요한 경우로서 본인의 동의를 얻기 어려울 때, 국가 기관 또는 지방 공공 단체 또는 그 위탁을 받은 자가 법령이 정하는 사무를 수행하는 것에 대해 협력 할 필요가 있는 경우이며, 본인의 동의를 얻는 것으로 해당 사무의 수행에 지장을 미칠 우려가 있을 때를 제외하고는 미리 외국의 제삼자에게의 제공을 인정하는 취지의 본인의 동의를 얻어야한다.[34] 이 경우에는 동조의 규정은 적용하지 아니한다.

31) 日置巴美・横澤田悠・本間貴明, 前掲論文, 時の法令 第1996號 (2016. 2.), 13-14頁; 横澤田悠, 前掲論文, 法律のひろば 第69卷 第5號 (2016. 5.), 18면

32) 일본의 역외에 있는 국가 또는 지역을 말한다. 개인의 권리 이익을 보호하기 위해 우리나라와 비슷한 수준에 있다고 인정되는 개인 정보 보호 제도를 가지고 있는 나라로 개인 정보 보호위원회 규칙으로 정하는 것을 제외한다

33) 개인 정보의 취급에 대해 이 절의 규정에 따라 개인 정보 취급 사업자가 강구해야 할 것으로 되는 조치에 상응하는 조치를 지속적으로 강구하는 데 필요한 것으로 개인 정보 보호위원회 규칙으로 정하는 기준에 적합한 체제를 정비하고 있는자를 제외한다.

34) 일본 개인정보보호법 제24조.

# 제3절 데이터 국지화(Data Localization) 해외 사례

데이터 국지화(Data Localization)은 자국민의 정보 주권을 보호하기 위하여 정보의 처리를 위한 서버를 자국 내에 두도록 강제하거나 자국내에서 처리하도록 제한하는 것을 말하는데, 이러한 데이터 국지화는 보통 자유로운 데이터의 국가간 이전과 대비되는 개념으로 사용된다. 데이터 국지화는 정보화 시대의 자유무역에도 역행하는 것으로 국가간 또는 다자간 무역협정을 체결하거나 협상할 때 논란의 대상이 되기도 한다. 이하에서는 데이터 국지화를 채택한 주요 국가로 소개되는 중국, 러시아, 캐나다를 비롯한 주요 국가의 사례를 살펴본다.

## Ⅰ. 중 국

중국은 “사이버공간의 주권과 국가안보, 사회공공이익을 수호하고 공민, 법인과 기타 조직의 합법적 권익을 보호하며 경제사회의 정보화의 건전한 발전을 촉진시키기 위해” 중화인민공화국 네트워크 안전법 (사이버안전법)을 제정 하였으며 이는 2017년6월 발효되었다.[35)]

사이버안전법은 네트워크 전반을 망라한 규제법으로서 네트워크에 대한 통제 강화 및 사이버공격에 대한 방어, 이와 더불어 중국이용자에 관한 정보를 보호하는 정부의 역량을 강화하기 위해 만들어진 법이다. 이 법은 네트워크 보안 지원과 촉진, 네트워크 운영 안전(제1절 일반 규정, 제2절 중요 정보 인프라의 운행 안전), 네트워크 정보 보안, 모니터링 경보와 비상 대응 등으로 구성되어 있어 ‘사이버 만리장성(Great Firewall)’을 구축하였다는 평가를 받고 있다. 이 법의 적용대상자는 네트워크운영자 , 핵심정보기반시설운영자 및 네트워크 상품 및 서비스 제공자이다.[36)37)]

35) 북경경도법률사무소(King&Capital Lawfirm), “중국 사이버보안법 관련 법규 해설”, 한국무역협회 북경지부 (2017.6.), 3면

36) - 네트워크사업자 : 네트워크 소유자, 관리자 및 네트워크서비스제공자
※ 네트워크을 정보의 수집・저장・전송・교환・처리를 위한 시설, 컴퓨터, 정보터미널 등의 시스템이라고 정의하

중국의 입법기관은 사이버보안법에 대하여 “사이버공간의 주권과 인터넷 상품/서비스 제공자의 안전의무를 명확히 하고 개인정보보호원칙을 세우고 핵심정보 인프라 안전보호 및 국경 간 전송규칙을 수립하였다”고 평가했다.[38)]

본 법률을 자세히 살펴보면, 핵심정보인프라시설 운영자가 중국내에서 운영하여 수집한 개인정보와 중요 데이터는 중국 내에 저장해야하고 업무수요로 중국경외로 송출하는 경우 국가인터넷정보부서와 국무원의 관련 부서가 제정한 방법에 따라 안전성평가를 진행해야 한다고(37조) 규정하여 개인정보 및 데이터 처리기준을 강화하였다. 또한 네트워크 보안 등급보호제도를 실시했으며(21조), 핵심정보인프라시설의 운영자는 반드시 자신의 네트워크의 안전성과 가능한 위험에 대해 해마다 최소 1회 검사평가를 진행해야 하며, 평가 상황과 개선조치를 해당 핵심정보인프라설비안전보호 담당 기관에 제출해야 한다(38조)는 규정 등을 통한 네트워크 보안 및 처리 과정 강화도 하였다.

## Ⅱ. 러시아

러시아는 스노든의 NSA 폭로 사건[39)] 이후, ‘디지털 주권(digital socereignty)’ 강화를 위해 입법제정을 한다. 러시아의 데이터국지화법은 2015년 9월 1일에 발효되었다. 러시아내에서 수집된 러시아인의 개인정보는 반드시 러시아 영토 내에 물리적으로 위치하고 있는 서버나 데이터베이스에 저장되거나 처리되어야만 하며 이러한 데이터국지화법은

---

고 있어 중국에서 사업목적으로 네트워크를 이용하는 모든 사업자가 포함되며 중국에 물리적으로 주재하지 않는 사업자도 포함

- 핵심정보기반시설운영자 : 핵심정보기반시설이란 공공통신, 정보통신, 서비스, 금융, 교통, 치수, 공공서비스, 전자정부 등 분실, 파손, 정보유출로 국민의 안전, 경제 또는 공공의 이익에 중대한 손해를 줄 수 있는 서비스를 제공하는 자
- 네트워크 상품 및 서비스 제공자 : 인터넷서비스 제공자, 유선전화, 휴대전화 운영자, 메신저 서비스 제공사업자

37) 김현경, “데이터 속성과 국지화 규범의 법적 쟁점에 대한 고찰”, 토지공법연구 제78집(2017.5.), 232면.

38) 북경경도법률사무소(King&Capital Lawfirm), “중국 사이버보안법 관련 법규 해설”, 한국무역협회 북경지부(2017.6.), 9면

39) 미 NSA 도청파문을 말한다. 즉, 전 미국 중앙정보국(CIA) 직원이자 미 국가안보국(NSA)에서 근무한 에드워드 스노든(Edward Joseph Snowden)이 2013년 6월에 NSA의 무차별적인 개인정보 수집 등의 내용을 담은 기밀문서를 폭로하면서 전 세계에 큰 파문을 일으킨 사건을 말한다.

러시아내의 자국민을 포함하여 러시아에 있는 외국회사 뿐만 아니라 러시아내에 주재하지 않더라도 온라인을 통해서 러시아로 물품을 배송하는 등 러시아시장을 타겟으로 하는 외국회사 또한 적용대상이다. 러시아인의 개인정보를 처리할 경우에는 반드시 러시아 정보보호국(Roskomnadzor)에 통지하여야 하고 러시아 정보보호국은 위법하게 처리된 정보에 대해서는 법원의 명령을 통해 웹사이트 차단 등의 접근제한 조치를 취할 수 있다.[40] 러시아 의회는 2016년 6월 기술 분야에 적용되는 반테러조치와 안보조치를 포함하는 연방법 개정안[41]을 통과시키는데, 이때 개정안에 포함된 러시아 정보법에 의하면 통신서비스제공자(CSP)와 인터넷을 통한 정보전달을 매개하는 사업자(FIDI)[42]는 인터넷 사용자와 고객 간의 음성, 문자, 사진, 비디오 등 기타 다른 유형 메시지와 같은 정보를 3년 동안 보관하여야 하고 통화와 문자메시지 내용을 6개월 동안 보관하여야 한다. 또한 암호화서비스를 제공하는 FIDI는 러시아 연방보안국(Russian Federal Security Service)에 해독키를 제공하여야 한다. CSP는 사이트 접속 내역에 관한 정보를 1년 동안 보관하여야 하며, 사법 당국의 요청이 있는 경우 정보를 제공해야 한다.[43]

## Ⅲ. 캐나다

캐나다의 개인정보 보호 및 전자문서법(the Personal Information Protection and Electronic Documents Act, PIPEDA)」은 캐나다 영역 밖으로 개인정보를 이전하는 것을 금지하고 있지는 않지만 지역 간 정보 이동에 대한 제한을 두고 있다. 이러한 지역 간 정보 이전 제한을 두게 된 이유는 미국에 기반을 둔 사업자들에게 지방정부의 정보기술 서비스를 아웃소싱하려는 시도에서 비롯되었다. 이러한 제한은 스노든 폭로 이전부터 이

40) 윤경선, “글로벌 인터넷 검열ㆍ통제 동향과 시사점”, 한국정보화진흥원(2017.10), 7면.

41) 개정안에는 러시아 통신법(No 126-FZ “On Telecommunications”과 정보법(No 149-FZ “On Information, Informational Technologies and Protection of Information”) 개정이 포함되어 있다.

42) FIDI란 인터넷 이용자의 전자메시지를 수신・송신・전송・처리하기 위해 디자인되거나 사용되는 정보시스템 또는 컴퓨터소프트웨어를 운영하는 자를 의미하며, 이에는 정보시스템을 운영하거나 메시지서비스 제공자, 공공이메일서비스제공자, 소셜미디어, 블로그, 뉴스 및 기타 플랫폼 등이 포함된다. (정보법 10.1(1))

43) 윤경선, “글로벌 인터넷 검열ㆍ통제 동향과 시사점”, 한국정보화진흥원(2017.10), 8면.

미 공식화되어 있었지만, 미국 애국법(USA PATRIOT Act)에 의해 미국의 감시가 심해지면서 오히려 더 정당하게 제한되고 있다. 두 개의 캐나다 주, 즉 브리티시 컬럼비아 주(British Columbia)와 노바 스코샤 주(Nova Scotia)는 정부 소유의 공공시설과 및 학교, 병원과 같은 공공 기관이 보유하고 있는 개인정보는 예외적인 경우를 제외하고 캐나다에서만 보관 및 접근할 것을  법률을 제정하였다. 브리티시 컬럼비아 주의 1996년 정보자유 및 프라이버시 보호법(Freedom of Information and Protection of Privacy Act)」에 의하면, 공공기관은 자신의 관리에 있거나 통제에 있는 개인정보가 캐나다 영역에서만 저장되고 접근가능 하도록 보장하여야 한다.[44] 다만 예외적으로 정보주체가 정보를 명확하게 인식한 상태에서 캐나다 외의 곳에서 정보에 대하여 저장 및 접근하는 것에 대하여 동의한 경우에만 허용이 되고 있다.

노바스코샤 주(Nova Scotia) 역시 유사한 개인정보 국지화 규정을 두고 있다.[45] 그러나 노바스코샤주 역시도 예외적으로 공공 기관의 운영을 위해 필요한 경우 공공기관의 장이 경정한 경우에만 캐나다 외의 곳에서 정보에 대한 접근 및 저장을 허용하고 있다.

앞서 살펴본바와 같이, 브리티시 컬럼비아 주가 규정하고 있는 법률에 따라 생각해본다면, 어떤 개인이 미국에 기반을 두고 있는 서비스인 구글의 Gmail을 사용할 경우 그 사람은 미국에서 개인정보를 이전하는 것에 대하여 동의해야하고 또한 Gmail을 이용하여 하는 대화내용 혹은 정보에 대하여 모든 캐나다 사람들 혹은 미국에 이러한 개인정보를 이전하는 것에 동의하여야만 한다.

44) Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, at c. 165, s. 30.1. ; 김현경, “데이터 속성과 국지화 규범의 법적 쟁점에 대한 고찰”, 토지공법연구 제78집(2017.5.), 238면(재인용)

45) Personal Information International Disclosure Protection Act, S.N.S. 2006, at c. 3, s. 5(1)(a) – b).; 30.1. ; 김현경, “데이터 속성과 국지화 규범의 법적 쟁점에 대한 고찰”, 토지공법연구 제78집(2017.5.), 238면(재인용)

## Ⅳ. 미 국

미국의 경우 '데이터 국지화'에 대해 법률로 제정하여 의무화 하고 있지 않지만, 데이터 주권 강화를 위해 다양한 노력을 하고 있다.

HIPAA를 통해 의료 데이터 사본에 대한 권리를 인정하고 활용 방안을 마련하고 있으며, '소비자 프라이버시[46] 권리장전'을 제정해 정보주체의 권리를 확대하고 있다. 또한 데이터 브로커들이 수집, 활용하는 데이터의 주체인 개인의 권리를 확대하기 위하여 노력하고 있다. 이렇듯 미국은 소비자 프라이버시 권리장전 등을 통해 개인이 가지고 있는 데이터 주권을 곧 소비자 권리라고 규정하여 데이터 산업을 발전시키기 위한 신뢰의 기반으로 삼아왔다.

또한 데이터 주권과 활용에 대한 인식제고를 위해 개인들에게 자발적으로 데이터 활용 과정에 참여하는 경험을 제공하는 시범 프로젝트 등을 추진하고 있다.[47]

미 의회조사국 CRS(Congressional Research Service)는 지난 6월에 발표한 '디지털 무역과 무역정책에 관한 보고서'에서 데이터 국지화가 기업들의 정보 수출을 방해하고, 국가간 금융거래에 장애가 됨으로써 기업 활동을 저지하기 때문에, 무역장벽으로 작용하고 있다고 발표하였고, 데이터 국지화가 다국적 기업의 운영을 어렵게 하고, 해외 각 나라의 별도 데이터 서버 시설의 구축으로 인해 기업의 운영비용 증가와 경쟁력의 저하를 초래한다고 평가하며 데이터 국지화에 대해 다소 부정적인 의견을 내놓았다. 현재 미국은 트래픽양에 따라 사용자의 인터넷 접속이 통신 공급자에 의해 달라질 수 있는 유럽과 달리 인터넷 공급자의 정보 필터, 사용자의 접속 차단 등을 금지하고 있다.[48]

---

46) 1890년에 Warren과 Brandeis가 논문에서 '프라이버시권은 진보된 문명세계에서 살고 있는 개인에게 필수적인 것'이라고 주장한 것이 프라이버시권의 역사적 유래라고 한다.(김진환, "개인정보 보호의 규범적 의의와 한계", 한국법학원, 저스티스 제144호,2014.10, 48면)

47) 한국정보화진흥원(NIA) 보도자료, "새로운 데이터 경제 시대, 데이터 주권의 부상", 2018.08.24.

48) 주로스앤젤레스 대한민국총영사관, "디지털 무역 이해하기 Ⅰ: 디지털 무역에서의 무역장벽" (2017.07) <http://overseas.mofa.go.kr/us-losangeles-ko/brd/m_4370/view.do?seq=1319204&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=> (2018.10.31. 최종방문)

# Ⅴ. 기 타

## 1. 베트남

데이터 국지화를 법으로 규정하는 국가들 중에서도 그 정도에 차이가 있는데, 베트남의 경우 인터넷 통화, SM서비스의 제공 및 이용의 관리에 관한 규정 및 정령72호를 통해 데이터 국지화에 대하여 강력하게 법으로 명문화 하여 규정하고 있다. ① 인터넷 통화, SM서비스의 제공 및 이용의 관리에 관한 규정(OTT[49]통달) 및 ② 정보기술 서비스 정령 사항을 살펴보면, 베트남 정보통신부(MIC)는 IT기기, 서비스에 대한 승인 및 등록과 데이터를 현지에 보관하는 것에 대하여 의무화 하는 정령의 제정을 추진하고 있다.

베트남에서는 2013년 정령 72호(No.72/2013/ND-CP)에 따라 일반 또는 사회관계망 웹사이트를 서비스하는 사업자는 베트남 감독당국의 검사를 받는 서버를 하나 이상 두어야 하며 데이터 보관 요건에 대해서도 규정하고 있는데 일반 웹사이트에 대해서는 적어도 일반 데이터를 사이트에 게시한 날로부터 90일 동안, 이미 처리한 정보의 로그 기록에 대해서는 2년 이상 동안 보관하여야 한다. 일반 웹사이트가 아닌 사회관계망 웹사이트의 경우에는 로그인과 로그아웃의 시간, 이용자 IP주소, 그리고 처리된 정보의 로그 기록을 2년 이상 보관하여야 한다. 테러나 범죄와 관련이 있거나 위법행위를 행했던 이용자에 대해서는 관할 행정청의 요구가 있을 경우 그의 인적 사항을 더불어 개인정보를 제공해야만 한다.[50] 2015년에는 공개정보의 국경간 제공을 규율하는 통달[51]의 시안이 공표되었다. 이때 공개정보의 국경간 제공이란 해외에 주재 하고 있는 기관 및 기업 또는 개인이 외국의 클라우딩 서비스를 이용하여 베트남 국내의 이용자에 대한 뉴스 웹사이트, SNS, 검색엔진 등 이용자가 열람 또는 다운로드 할 수 있는 공개정보에 관련한 어플 등을 제공하거나 하드웨어를 설치하는 경우를 통틀어 일컫는다. 이에 따라 뉴스 사이트, 검색엔진

49) Over the Top에서 Top은 TV셋톱박스 같은 단말기를 뜻하므로 OTT는 셋톱박스 같은 단말기를 넘어서서 인터넷과 모바일을 이용한 영화, 방송, 교육 등 각종 미디어 콘첸츠를 제공하는 서비스를 말한다.

50) Scott Livingston and Graham Greenleaf, “Data localisation in China and other APEC jurisdictions”, Privacy Laws & Business International Report Issue 143, October 2016, pp. 6-7

51) Draft circular on detailed regulation on cross border provision of public information(No.72/2013/ ND-CP)

등을 국외의 하드웨어 또는 클라우딩 서비스를 이용하여 운영을 하는 경우, SNS에 가입되어있는 회원이 5천명을 넘을 경우에는 법적인 대표자가 베트남 국내에 있어야 한다. 예외적으로 순전히 상업적인 웹사이트로서 특성화된 응용(specialized application) 사이트인 경우에는 데이터 처리 및 보관의 현지화 의무가 없다. 예를 들면, 통신, 정보기술, 방송, 텔레비전, 상거래, 금융, 은행, 문화, 헬스케어, 교육 기타 일반적인 정보제공이 아닌 전문 분야에 속한 웹사이트가 이에 해당한다.[52]

### 2. 호 주

호주의 경우 데이터 국지화, 즉 데이터 해외 이전에 대한 정도가 다른 나라들에 비하면 심한 편은 아니다. 특정 분야에 한해서만 제한을 하고 있는데, 그 예로 헬스케어, 이동통신, 금융, 국가안보 등과 같은 야에 한하여 정보의 국외 이전을 제한하고 있고 개인정보보호법 등은 일정종류의 정보는 반드시 국내 서버에 저장하고 처리할 것을 의무화 하고 있다.

특히 대표적인 예로, 전자적 형태인 개인건강정보기록을 호주 밖으로 송출 되는 것을 막고 있다. 등록된 포털 운영자 또는 등록된 계약 서비스 제공자인 건강기록 시스템 운영자는 비식별 처리가 되지 않은 개인 식별 가능한 호주시민의 건강기록에 대해서 해외, 보관, 처리하는 것을 금지하고 있다. 때문에 개인을 식별할 수 있는 정보가 포함되어 있지 않는 경우에는 호주 영토 밖으로 이전되거나 처리되는 것이 허용된다. 즉, 호주에서 건강관련 정보를 취급하는 외국기업은 데이터센터를 호주에 설립하거나 호주에 설립되어 있는 기업의 아웃소싱을 통해서만 건강관련 정보를 취급할 수 있는 것이다.[53]

### 3. 브라질

브라질은 일정한 조건하에서만 정보의 국외 이전을 제한하고 있는데, 브라질 호세프

52) 박훤일, “개인정보의 현지화에 관한 연구”, 경희대학교 법학전문대학원, 경희법학52권4호(2017.12), 23면
53) 김현경, “데이터 속성과 국지화 규범의 법적 쟁점에 대한 고찰”, 토지공법연구 제78집(2017.5.), 239면

대통령은 미국을 우회하는 남미와 유럽 간의 정보통신망을 연결하는 해저 광섬유 케이블 설치 계획을 제안하면서, 브라질 우정국에 암호화된 이메일 시스템 개발을 지시하였다.[54] 의회에 대해서는 구글, 마이크로소프트 등 미국의 IT기업들이 브라질 이용자에 대한 데이터를 국내 서버에 보관할 것을 의무화 하는 법 개정을 촉구하였다. 이러한 움직임은 인터넷 트래픽이 미국을 경유하지 않도록 하고 데이터를 브라질 내에서 보존하도록 한다면 브라질 정부가 브라질 국민들의 개인정보 및 그 외 데이터에 대해 더 안전하게 보호할 수 있다는 생각에 근거한 조취라 볼 수 있다. 그러나 NSA(National Security Agency; 미국 연방 정부의 해독 첩보국)와 같은 외국 정보기관이 브라질 국민들의 인터넷을 통한 활동을 감시하는 것을 전면적으로 막을 수는 없으며 이와 같은 조치가 브라질 국내의 정치적 상황에 대한 고려에서 시도된 측면도 있음을 지적하는 견해도 있다.[55]

## 제4절 외국인 개인정보 열람에 관한 해외 법제 조사

### Ⅰ. EU의 개인정보보호법(GDPR)

#### 1. GDPR의 배경

2018년 5월25일부터 시행되는 EU의 개인정보보호법인 GDPR(General Data Protection Regulation)은 단순히 개인정보 보호 강화 목적만이 아닌 빅데이터 활용기반을 확대하는 법제로 볼 수 있다.

“EU는 미국 중심으로 진행되고 있는 4차 산업혁명의 주도권을 회복하고 저성장 돌파구를 모색하기 위해 전 경제, 산업의 디지털화를 통한 ‘디지털 단일시장 전략’을 추진하

54) 허진성, “데이터 국지화(Data Localization) 정책의 세계적 흐름과 그 법제적 함의”, 언론과 법 제13권 제2호(2014.12.), 296면.

55) Amar Toor, Cutting the cord: Brazil’s bold plan to combat the NSA, <http://www.theverge.com/2013/9/25/4769534/brazil-to-build-internet-cable-to-avoid-us-nsa-spying> (2018.10.31. 최종방문) ; 허진성, “데이터 국지화(Data Localization) 정책의 세계적 흐름과 그 법제적 함의”, 언론과 법 제13권 제2호(2014.12.), 296면.

고 있으며 이를 위해 모든 회원국에 일괄 적용되는 '일반 개인정보보호법(GDPR)'을 마련하여 EU 기업의 규제 비용을 줄이고  EU내 전자상거래 활성화를 촉진시키기 위해 제정하였다. 단, EU외에 있는 기업도 EU의 법규를 준수해야 하는 부담이 발생한다."[56]

## 2. 주요원칙

정보주체가 동의했거나, 정보주체와의 계약 이행이나 계약 체결을 위해 필요한 처리, 법적의무 이행을 위한 처리, 정보주체 또는 다른 사람의 중대한 이익을 위해 필요한 처리, 공익을 위한 임무의 수행 또는 기업에게 부여된 공적 권한의 행사를 위해 필요한 처리, 기업 또는 제3자의 적법한 이익 추구 목적을 위해 필요한 처리 일 경우 개인정보를 적법하게 수집, 이용 제공을 할 수 있으며 정보주체의 명시적 동의가 있는 경우 또는 회원국 법률에 따른 경우 등을 제외하고는 민감 정보의 처리는 원칙금지[57]하고 있다.[58]

## 3. 적용대상

EU에서 사업장을 운영하거나 EU 내에 사업장은 없으나 인터넷 홈페이지 등을 통하여 EU 거주민들에게 물품 또는 서비스를 제공하는 경우도 포함되며 EU 주민의 행동을 모니터링 하는 기업 등이 GDPR의 적용을 받는다.[59]

56) 한국인터넷진흥원(KISA), <https://www.kisa.or.kr/business/gdpr/gdpr_tab2.jsp> (2018.10.31. 최종방문)

57) 민감정보의 범위 : 인종・민족, 정치적 견해, 종교・철학적 신념, 노동조합의 가입여부를 나타내는 개인정보의 처리와 유전자 정보, 자연인을 고유하게 식별 할 수 있는 생체정보, 건강정보, 성생활・성적 취향에 관한 정보의 처리는 금지한다.
① 정보주체의 명시적 동의(explicit consent)의 경우 등 ② 고용, 사회안보나 사회보장법 또는 단체협약에 따른 의무의 이행을 위해 필요한 경우 ③ 정보주체가 일반에게 공개한 것이 명백한 경우 등 에 해당하면 민감 정보 처리가 가능하다.

58) 행정안전부・방송통신위원회・한국인터넷진흥원, 우리 기업을 위한 EU 일반 개인정보보호법 가이드북, 2018

59) GDPR 제3조.

### 4. 규정사항

규제(EU) 2016/679[60], EU(EU) 의 새로운 일반 정보 보호 규정(GDPR)은 EU 내 개인, 회사 또는 EU에 살고 있는 개인과 관련한 데이터를 처리하는 기관을 규제한다. 이 규정은 전문 활동이나 상업적 활동과 관련이 없을 경우, 개인이 처리 한 데이터에는 적용되지 않는다. 개인이 사회 문화적 또는 금융활동을 위해 개인 데이터를 사용하는 경우 데이터 보호법을 준수해야한다. 예를 들면, EU에 설립 된 회사가 발트 해 국가를 기반을 둔 고객에게 여행 서비스를 제공하며, 그 맥락에서 자연인의 개인 데이터를 처리하는 경우 이 규정이 적용된다.[61]

### 5. GDPR에서의 데이터

개인데이터란 식별되거나 식별 가능한 개인과 관련된 모든 정보를 의미한다. 개인 식별이 불가능하거나(익명데이터) 암호화되었지만(가명데이터) 개인 식별을 위해 사용될 수 있는 데이터는 개인 정보로 남아 있으며 법의 범위 내에 속한다. 개인을 더 이상 식별할 수 없거나 더 이상 식별할 수 없는 방식으로 익명 처리된 개인 데이터는 더 이상 개인 데이터로 간주되지 않는다. 익명화 된 데이터의 경우 익명화는 되돌릴 수 없어야 한다. 이 법은 해당 데이터를 처리하는 데 사용되는 기술에 관계없이 개인 데이터를 보호한다. 사전 정의된 기준(예 : 사전 순)에 따라 데이터가 정리된 경우 자동 중립 및 수동 처리 모두에 적용된다. 또한 IT 시스템, 비디오 감시 또는 용지를 통해 데이터가 저장되는 방식과는 상관없이, 모든 경우에 있어 개인 정보는 GDPR에 명시된 보호 요구 사항의 적용을 받는다.[62]

---

60) Regulation (EU) 2016/679 of the European Parliament and of the Councilof 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 (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

61) Articles 1 and 2 and Recitals (1), (2), (14), (18) and(27) of the GDPR.; 유럽위원회(European Commission), https://ec.europa.eu

62) Articles 2, 4(1) and(5) and Recitals (14), (15), (26), (27), (29) and (30) of the GDPR.

데이터 처리는 수동 또는 자동화 된 방법을 포함하여 개인 데이터에 대해 수행되는 광범위한 작업을 일컫는다. 여기에는 개인 데이터의 수집, 기록, 조직, 구조화, 저장, 적응 또는 변경, 검색, 상담, 사용, 공개 또는 전송, 배포, 조정 또는 결합, 제한, 삭제 또는 파기 등이 포함된다. GDPR(General Data Protection Regulations)은 구조화 파일링 시스템의 일부인 경우 자동적인 수단과 비자동적인 처리에 의해 전적으로 또는 부분적으로 개인 데이터 처리에 적용된다.[63]

이러한 GDPR은 '익명 데이터'와 '가명 데이터'를 사용할 수 있게 규제하고 있으며 이는 기업에게 비식별 조치가 이루어진 개인정보에 대해 접근하고 활용할 수 있게 허용해 준 법안이라 할 수 있다.

## Ⅱ. 미국 수사기관의 정보수집권에 관한 법률

### 1. 2001년 애국법 (PATRIOT Act)

미국은 지난 9·11 사태 이후 테러와의 전쟁을 선포하고 이를 지원하기 위하여 국토안보법(Homeland Security Act)과 애국법(USA PATRIOIT Act of 2001; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism of 2001)과 같은 새로운 법률을 제정하고 이에 따라 기존의 다른 법률들도 관련 부분에 대한 개정을 하게 되었다. 연방정부는 테러범을 색출하여 체포하거나 테러를 시도하는 것을 방지하기 위하여 테러관련 개인정보 수집에 대한 권한강화를 시도하였다.[64]

애국법은 테러행위에 대한 수사와 정보 수집을 담당하는 법집행기구 그리고 정보공동체의 국 · 내외에서의 권한을 대폭 확대하여 테러범죄에 대한 효율적인 수사와 정보수집을 위해 적법절차를 극적으로 완화하는 것을 골자로 한다. 국가비상사태가 발생할 경우

63) Article 4(2) and(6) of the GDPR.
64) 오길영, "클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률안의 검토와 비판", 민주주의법학연구회, 민주법학 56권0호(2014.11.), 463면.

궁극적으로 범죄 및 사건을 마무리할 수사업무와 이러한 사건 및 테러를 사전에 방지하기 위한 필요한 조치를 포함하여 형사적 대처업무를 주된 내용으로 하고 있다. 65)

Joe Biden (D-DE) 상원 의원은 “FBI는 마피아를 조사하기 위해 도청을 할 수 있지만 테러리스트를 수사할 수는 없었다”라고 말했다. 이처럼 애국자법을 통해 수사관들은 조직범죄 및 마약 밀매를 조사할 수 있게 되었고 휴대전호와 같은 정보 통신 장치를 이용하여 감시를 방해하는 국제 테러리스트들의 급속한 변화에 발맞춰 이러한 테러리스트들을 추적하기 위해 국가보안 수사는 이 법을 통해 들키지 않고 조사를 수행할 수 있게 됐다. 또한 이 법안은 법 집행 기관, 정보 기관 및 국방 공동체가 미국 국민과 국가 안보를 보호하기 위해 자신의 업무를 공개하고 조정하는 것을 방해하는 주요 법적 장벽을 제거했다. John Edwards (DN.C.) 상원 의원이 애국법에 관해 “우리 정부의 오른손이 왼손이 무엇을 하는지 모른다면 우리는 단순히 테러와의 전쟁에서 승리 할 수 없다”(Press release, 10 / 26/01)라고 언급한 바와 같이 애국법을 통해 경찰관, FBI 요원, 연방 검찰 및 정보 관리는 테러 분자가 완성되기 전에 테러 분자를 밝히기 위해 “도트를 연결”함으로써 우리 공동체를 보호 할 수 있게 되었다.66)

특히 정보와 수사기관이 전화, 전자 우편, 각종 통신, 금융 의료를 비롯한 각종 기록을 검색하고 접근하는 것에 대한 제한을 대폭 완화했으며 미국 내에서 해외 정보수집에 대한 대폭적인 제한 완화, 외국인 개개인 및 단체들의 금융거래에 대한 감시와 통제에 대한 재무부 장관의 권한 확대, 테러 관련 용의자에 대한 구금을 함에 있어서 이민국을 포함한 법집행 당국의 재량권의 대폭적인 확대를 골자로 한다. 67)

그러나 애국법은 신속한 수사 및 테러공격의 예방을 위해 만들어진 법이지만 헌법상의

65) 한희원, “초국가적안보위협세력에의 법규범적 대응 법제연구 : 미국 애국법에 대한 고찰”, 중앙법학회, 중앙법학 12권2호(2012.6.), 97면.

66) M Department of Justice, Highlights of the USA PATRIOT Act, <http://www.justice.gov/archive/ll/highlights.htm> (2018.10.31. 최종방문).

67) 한희원, “초국가적안보위협세력에의 법규범적 대응 법제연구 : 미국 애국법에 대한 고찰”, 중앙법학회, 중앙법학 12권2호(2012.6.), 97면.

시민들의 권리를 지나치게 제약하거나 침해할 수 있다는 비난도 받으며 2015년 6월 결국 폐기됐다. 미국 정부와 의회가 부작용이 지나친 애국법을 폐지하고 독소 조항[68]을 제거한 '미국 자유법(USA Freedom Act, 본 명칭은 Uniting and Strengthening America by Fulfilling Rights and Ensuring Affective Discipline over Monitoring Act, Public Law 114-23)'을 새로 만든다. 이 법은 애국법 제215조와 같은 광대한 미국시민에 대한 정보나 수사기관의 통신기록의 수집을 못하도록 했고, 테러나 간첩(espionage)수사에 필요한 통신자료만을 통신기관이 5년간 보관하도록 했다. NSA나 기타 수사기관이 통신 기록을 확보하려면 법원의 영장을 받도록 되어있다. 이러한 미국 자유법은 애국자법에서 자유법으로 이름은 새롭게 수정하였으나 그 내용은 애국자법 제 215조를 약간 수정하여 계승하였다고 볼 수 있다. 특히 애국자법이 규정한 외국과 관계없는 자생적 테러(lone wolf)나 수시로 통신번호를 바꾸는 테러 용의자를 감청하는 권한은 그대로 유지하였다. 외국 정보에 대한 감청 및 수사는 미국 자유법 이외에 주로 1978년에 제정한 외국정보감시법(Foreign Intelligence Serveillance Act이고, 약칭은 FISA이다. 연방공법 95-1783)에 따른다. 이 법은 외국이나 외국의 대리인(Agents) 간의 정보 통신, 기타 통신을 수집하는 합법 절차를 규정한 것이다. 외국을 위하는 간첩이나 테러용의자는 미국인일 수도 있다. 만약 미국인이 연관된 일이 발견되었을 경우에는 감청이 가능하나 감청이 시작된 후 72시간 내에 법원의 영장을 획득하여야한다.[69]

### 2. 2015년 자유법 (FREEDOM Act)

미국 연방의회는 '애국자법'의 주요 규정들에 대해서 연장하는 대신 '권리 실현 및 감시에 대한 효과적 통제 확보를 통한 미국 통합과 강화를 위한 법률'(Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring

68) 애국법에서 특히 문제가 되었던 조항은 215조인데, 스노든 폭로 당시 NSA가 개인 정보를 무차별 수집활동이 바로 애국법 215조를 근거로 했기 때문이다. 215조는 외국 정보 수집이나 국제 테러 수사에 필요한 경우, 미 정보 당국이 기업이나 개인 정보를 취득할 수 있게 허용하는 내용을 담고 있고 이는 영장을 필요로 한다.

69) 이종연 미국변호사, "미국 현행 통신 감청법 제도와 절차", 법률신문 오피니언(2015.08.13.자), <https://www.lawtimes.co.kr/Legal-Opinion/Legal-Opinion-View?serial=94910> (2018.10.31. 최종방문)

Act of 2015) 즉 '미국 자유법(USA FREEDOM Act of 2015)'을 제정한다. 애국법이 테러 방지를 위한 정보기관의 감시 및 해외첩보 권한 강화 법률이라면, 자유법은 '사생활보호법'에 가까워 정보기관의 수사권을 제한하는 법이라고 볼 수 있다. 그러나 '애국법'의 일부 규정들만 개정하고, 대부분의 규정들은 유효하게 존속하기 때문에 '자유법'의 효과에는 제한이 있을 수밖에 없다. 대신 엄격한 절차 하에 '긴급한 상황 발생 시' 법원의 명령 없이도 통화내역기록의 제공을 요구할 수 있는 권한을 법무부장관에게 부여하는 신규 규정이 마련되었으며, 일체의 통화내역기록이나 유형물(책자, 기록, 서류, 문서 등)들을 수집하기 위해서는 '특정선별용어'를 반드시 사용하도록 의무화하여 정보수집의 대상을 한정하고 이로써 정보기관들이 통신자료 수집행위를 무분별하게 하지 못하게 저지하고 일반인들의 사생활 보호 권리를 강화하고자 하였다.[70]

### 3. 2018년 클라우드법(CLOUD Act)

최근 미국에서 발표된 '해외 데이터 이용 합법화(The Clarifying Lawful Overseas Use of Data)' 즉, '클라우드 법(CLOUD Act.)'은  미국 수사기관이 구글이나 마이크로소프트, 애플 등과 같은 IT기업들의 해외 서버에 저장된 메일, 문서와 같은 기타 통신 자료 등을 열람할 수 있도록 권한을 부여하고 있다. 이 법이 실행되면 미국 수사기관은 법원의 압수수색 영장을 따로 발부받지 않더라도 해외서버에 저장된 미국기업들의 데이터를 감청할 수 있으며, 데이터가 어디에 있던지 필요한 개인정보 데이터 수집이 가능하게 된다.[71]

이러한 클라우드 법이 만들어지게 된 배경에는, '마이크로소프트 이메일 사건'[72]이 있다. 이 사건을 계기로 '해외저장데이터 획득에 관한 법(Law Enforcement Access to Data

70) 최창수, "수사ㆍ정보기관의 통신이용 정보수집권에 관한 미국의 입법례와 그 함의 - 「2015년 미국 자유법」에 대한 검토를 중심으로-, 한국정보법학회, 정보법학 제20권 제1호(2016.05.), 131면,134면

71) 백지영, "美, 클라우드법 발효...사생활 침해vs공익 충돌 우려", 디지털데일리, 2018.03.27. 기사, <http://www.ddaily.co.kr/news/article.html?no=167178> (2018.10.31. 최종방문) 참조.

72) 2013년 12월, 마약밀매사건의 수사를 위해 마이크로소프트사에 범죄와 연루된 특정 이메일 계정에 관련한 데이터 및 관련 이메일의(이메일 서버는 미국이 아닌 아일랜드였다.) 제출을 요구하는 영장을 신청했는데, 마이크로소프트가 이의를 제기하여 소송까지 간 사건이다.

Stored Abroad Act, 2015)'과 '국제통신 개인정보보호법'(International Communications Privacy Act, 2017)을 합쳐서 만든 법률이 바로 클라우드법인 것이다. 클라우드법을 자세히 알아보기전, 우선 마이크로소프트 사건의 쟁점 법률이자 클라우드법의 입법 배경인 저장통신법(Stored Communication Act) 2703조의 내용을 알아보고자 한다.

저장통신법에 의하면 180일 이내에 저장된 정보에 대해서는 영장을 발급 받아야 하며[73] 180일 이상 보관된 경우, 정부는 범죄수사와 관련이 있다는 "구체적이고 명백한 사실"을 바탕으로 행정명령이나 법원명령을 통해 사전 통고 없이 정보를 입수할 수 있다.[74] 수색영장 집행에 있어 일반적인 경우 영장 집행 시 법집행관이 영장집행 장소에 반드시 임장해야 하지만, 본조에 따르면 이 법에 따른 영장 집행시에는 법징행관의 임장이 요구되지 않는다고 명시적으로 규정하고 있다.[75] 덧붙여, 한 연방 항소법원은 저장통신법이 치외법권적으로 적용되지 않는다고 판결하였는데 이는 정부가 독점적으로 외국 서버에 저장된 전자메일 컨텐츠를 점유할 영장을 얻을 수 없다는 것을 의미한다.[76]

앞서 밝힌바와 같이 클라우드 법은 법집행기관의 수사에 대한 장벽을 없애는 것에 있다. 테러리즘을 포함한 심각한 범죄에 신속하고 정확하게 대응하기 위해서는 통신서비스 제공자가 보유하고 있는 데이터에 적시에 접근하는 것이 필요했으나 그간 이러한 데이터 서버가 해외에 있는 경우 데이터데 대한 접근이 어려웠다. 클라우드 이전의 저장통신법에는 정보서비스제공자에게 미국 외에 저장되어 있는 데이터의 제출을 요구할 수 있는지에 대한 여부가 명시적으로 규정되어 있지 않았다. 이에 '마이크로소프트 사건'과 같은 문제가 발생하기에 이른다. 그리고 이러한 문제들을 해결하기 위하여 클라우드 법이 제정된 것인데, 클라우드 법 제2713조를 살펴보면 "서비스제공자는 해당 통신, 기록 또는 기타 정보가 미국 내 또는 미국 밖에 저장되어 있는지 여부와 관계없이 해당 제공자가 보유,

73) 18 U.S.C. § 2703(a)

74) 18 U.S.C. § 2703(b), § 2703(d) ; Jennifer R. Henrichsen and Hannah Bloch-Wehba, "electronic commuications survellance : what journalist and media organizations need to know", reporters committee, p.10

75) 18 U.S.C. § 2703(g)

76) In Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 216 (2d Cir. 2016).

보관 또는 통제하고 있는 유선 또는 전자통신의 내용 및 기타 기록 또는 고객 또는 가입자의 정보를 보존, 백업(backup), 또는 공개할 법적 의무를 준수하여야 한다."[77]라고 규정함으로서 미국 수사당국이 미국 내에 존재하지 않는 정보에 대해서도 접근할 수 있도록 명시하였다.[78]

77) 18 U.S.C. § 2713. Required preservation and disclosure of communications and records "provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider' possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

78) 송영진, "미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점", 한국형사정책연구원, 형사정책연구제29권 제2호(통권114호, 2018.), 157면.

korea
legislation
research
institute

# 제3장
# 해외에서의 우리 국민의 개인정보 처리에 관한 현행법상의 규율 분석

# 제3장 해외에서의 우리 국민의 개인정보 처리에 관한 현행법상의 규율 분석

## 제1절 현행법 상 개인정보 국외이전 규정 검토

### Ⅰ. 개인정보보호법

> **제17조(개인정보의 제공)** ③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

개인정보에 관한 일반법이라고 할 수 있는 개인정보 보호법은 제 17조에서 개인정보의 국외 제3자 제공에 대하여 규정하고 있다. 즉, 개인정보처리자가 개인정보를 국외의 제3자에게 '제공'하고자 할 때에는 ① 개인정보를 제공받는 자의 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처, ② 제공받는 자의 개인정보 이용 목적, ③ 제공하는 개인정보의 항목 ④ 제공받는 자의 개인정보 보유 및 이용 기간, ⑤ 동의 거부권이 존재하다는 사실 및 동의 거부에 따른 불이익이의 내용(불이익이 있는 경우에 한함)을 모두 정보주체에게 알리고 동의를 받아야 한다. 국내외를 불문하고 개인정보를 제3자에게 제공할 때에는 동의를 얻어야 할 의무와 고지의무가 부과되어 있으며 이법을 위반하는 내용으로는 개인정보의 국외 이전에 관한 계약을 체결할 수 없도록 하고 있는데 이는 개인정보를 국외로 이전하여 이법의 적용을 회피할 수 없도록 하기 위함이다.[79]

79) 행정안전부, "개인정보 보호법령 및 지침·고시 해설"(2011. 12), 97면.

다만 이 법은 개인정보의 국외 이전 전체를 포함하는 것이 아니라 국외의 제3자에게 '제공'하는 경우만을 규율하고 있어 개인정보의 처리를 국외의 제3자에게 위탁하거나, 영업의 양도・합병 등에 의하여 개인정보 데이터 베이스가 국외로 옮겨지는 등의 경우에는 해당되지 않는다. 예를 들면 국외에 자회사를 설치하고 고객의 개인정보를 이용해 업무를 하도록 하는 경우나 국내의 기업이 외국 기업과 합병하여 국내 고객의 개인정보의 데이터 베이스가 국외로 옮겨지는 경우를 말한다.

이 법에 따라 정보주체의 동의를 받지 않고 개인정보를 국외의 제3자에게 제공한 자 또는 그 사정을 알고 제공받은 자는 5년 이하의 징역 또는 5천만원 이하의 벌금(제71조제1호), 정보주체에 대한 고지의무를 위한한 자는 3천만원 이하의 과태료(제75조제2항제1호)가 부과된다.

## Ⅱ. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법"이라 한다) 제63조는 정보통신서비스 제공자 등이 이용자의 개인정보를 국외로 이전하기위해서는 이용자의 동의를 받아야 한다고 규정하고 있다. 제63조에 의하면 정보통신 서비스제공자 등은 이용자의 개인정보를 국외로 제공(조회되는 경우를 포함한다)・처리위탁・보관(이하 이 조에서 "이전"이라 한다)하려면 ① 이전되는 개인정보 항목, ② 개인정보가 이전되는 국가, 이전일시 및 이전방법, ③ 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처) ④ 개인정보를 이전받는 자의 개인정보 이용목적 및 보유・이용 기간을 이용자에게 고지하고 동의를 받아야 하며, 이 법을 위반하는 사항을 내용으로 하는 계약을 체결하여서는 안 된다.

개인정보의 국외 제3자 제공에 관해서만 규정하고 있는 개인정보보호법과는 달리 정보통신망법에서는 국외 제3자 제공 뿐 아니라 위탁, 보관 등의 모든 국외이전을 포함하고 있다. 따라서 국외에 데이터센터를 두고 국내에서 개인정보를 수집・이용・가공하는 때에도 원칙적으로 이용자의 동의를 받아야 한다.

다만, 제2항 단서에 따르면 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제3항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁 · 보관에 따른 동의절차를 거치지 아니할 수 있다.

또한 정보통신서비스 제공자등은 정보주체의 동의를 받아 개인정보를 국외로 이전하는 경우에도 대통령령으로 정하는 바에 따라 보호조치를 취해야 한다고 규정하고 있다(제63조 제4항). 그런데 유럽연합의 개인정보보호 법제의 경우 국외이전을 할 자와 받을 자가 공동으로 이러한 보호조치를 하도록 하고 있고 또한 이러한 보호조치를 이행하면 국외이전에 대해 이용자의 동의를 받지 않아도 된다고 규정하고 있는데 반해 정보통신망법은 정보통신서비스 제공자가 국외이전에 대한 동의와 함께 보호조치를 해야한다는 차이점이 있다.[80]

**제63조(국외 이전 개인정보의 보호)** ① 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니 된다.

② 정보통신서비스 제공자등은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다) · 처리위탁 · 보관(이하 이 조에서 "이전"이라 한다)하려면 이용자의 동의를 받아야 한다. 다만, 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제3항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁 · 보관에 따른 동의절차를 거치지 아니할 수 있다.

③ 정보통신서비스 제공자등은 제2항에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.

1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유 · 이용 기간

80) 이창범, "한국의 개인정보 국외이전 법제 현황과 개정방향", 법학논총 제36권 제3호, 전남대학교 법학연구소(2016), 376면.

④ 정보통신서비스 제공자등은 제2항에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

**제63조(국외 이전 개인정보의 보호)** ① 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니 된다.

② 정보통신서비스 제공자등은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 조에서 "이전"이라 한다)하려면 이용자의 동의를 받아야 한다. 다만, 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 제3항 각 호의 사항 모두를 제27조의2제1항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁·보관에 따른 동의절차를 거치지 아니할 수 있다.

③ 정보통신서비스 제공자등은 제2항에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.

1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간

④ 정보통신서비스 제공자등은 제2항에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

⑤ 이용자의 개인정보를 이전받는 자가 해당 개인정보를 제3국으로 이전하는 경우에 관하여는 제1항부터 제4항까지의 규정을 준용한다. 이 경우 "정보통신서비스 제공자등"은 "개인정보를 이전받는 자"로, "개인정보를 이전받는 자"는 "제3국에서 개인정보를 이전받는 자"로 본다.

**제63조의2(상호주의)** 제63조에도 불구하고 개인정보의 국외 이전을 제한하는 국가의 정보통신서비스 제공자등에 대하여는 해당 국가의 수준에 상응하는 제한을 할 수 있다. 다만, 조약 또는 그 밖의 국제협정의 이행에 필요한 경우에는 그러하지 아니하다.

한편 2019년 3월 시행을 앞두고 있는 신설 규정이 있는데, 제63조제5항과 제63조의2가 그것이다.

먼저 제63조제5항은 국외로 이전된 개인정보를 다른 국가로 재이전 하는 경우에 개인정보 국외이전과 동일하게 원칙적으로 이용자의 동의를 받아야 하고(예외적으로 계약의 이행을 위하여 필요하고 이용자의 편익을 증진시키는 경우에는 개인정보 처리방침을 통한 공개), 개인정보 보호조치를 취하여야 한다고 규정하고 있다.

이는 글로벌 기업이 국내 이용자의 개인정보를 해외로 이전한 후 제3국으로 재이전하는 등 해외 시장에서 유통하고 있음에도 기존의 정보통신법에서는 이를 명확하게 규제할 근거가 마련되어 있지 않다는 필요성에 따라 마련되었다.[81]

또한 개인정보 보호 수준이 다른 나라들로 우리 국민의 개인정보가 이전되는 경우에도 안전하게 유통될 수 있도록 합리적이고 탄력적으로 대응할 필요성을 고려하여 제62조의2 상호주의 규정을 도입하였다.[82]

## Ⅲ. 신용정보의 이용 및 보호에 관한 법률

신용정보의 이용 및 보호에 관한 법률(이하 신용정보법이라한다)은 신용정보의 국외이전 절차에 대해 규율하고 있지 않고 개인신용정보의 제3자 제공에 관한 사항을 규정하고 있는데, 이 법 제32조 제1항에서는 신용정보제공 또는 이용자가 개신신용정보를 다른 사람에게 제공하려는 경우에는 ① 개인신용정보를 제공받는 자, ② 개인신용정보를 제공받는 자의 이용 목적, ③ 제공하는 개인신용정보의 내용, ④ 개인신용정보를 제공받는 자(신용조회회사 및 신용정보집중기관은 제외)의 정보 보유 기간 및 이용 기간을 해당 신용정보주체에게 고지하고, 개인신용정보를 제공할 때마다 개별적 동의를 받도록 하고 있다.

81) 이러한 국외 개인정보 재이전에 대한 규정은 GDPR의 규정을 참고하여 도입되었다고 평가된다. GDPR에서는 국외 개인정보 재이전에 대하여 따로 규정을 두고 있는 것은 아니고 국외이전에 관한 조항들에 재이전을 포함하고 있는데 따라서 국외이전의 허용기준(제45조 적합성 평가)이나 예외적 허용에 관한 사항(제47조 BCPs 등)이 그대로 준용된다. 최경진, “GDPR등 EU와 우리나라 온라인상 개인정보보호 법제 비교 연구”, 방송통신정책 연구 연구보고서, 방송통신위원회(2016), 127-128면.

82) 이 외에도 해외 사업자가 국내에 정보통신서비스를 제공할 때에는 국내 주소 또는 영업소가 없다면 대리인을 지정하도록 하고 국내 대리인은 개인정보 보호책임자의 업무(이용자의 고충 처리 등), 개인정보 유출등의 통지・신고 및 지체 사유 소명, 조사에 필요한 자료제출 등의 업무를 수행하도록 하였다.(제32조의5 신설)

**제32조(개인신용정보의 제공 · 활용에 대한 동의)** ① 신용정보제공 · 이용자가 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 다음 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공할 때마다 미리 개별적으로 동의를 받아야 한다. 다만, 기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성 · 최신성을 유지하기 위한 경우에는 그러하지 아니하다.

1. 서면
2. 「전자서명법」 제2조제3호에 따른 공인전자서명이 있는 전자문서(「전자거래기본법」 제2조제1호에 따른 전자문서를 말한다)
3. 개인신용정보의 제공 내용 및 제공 목적 등을 고려하여 정보 제공 동의의 안정성과 신뢰성이 확보될 수 있는 유무선 통신으로 개인비밀번호를 입력하는 방식
4. 유무선 통신으로 동의 내용을 해당 개인에게 알리고 동의를 받는 방법. 이 경우 본인 여부 및 동의 내용, 그에 대한 해당 개인의 답변을 음성녹음하는 등 증거자료를 확보 · 유지하여야 하며, 대통령령으로 정하는 바에 따른 사후 고지절차를 거친다.
5. 그 밖에 대통령령으로 정하는 방식

이처럼 동법의 제3자 제공이 국내의 제3자라고 규정되어 있지 않으므로 국외의 제3자 제공에도 해당한다고 해석한다면 이 법의 규정을 받을 수 있고, 만일 이에 관하여 신용정보법에 개인신용정보의 국외이전에 관한 직접적인 명문 규정이 없어 이법의 적용범위에 포함되지 않는다고 하더라도 개인정보에 관하여 개인정보보호법이 일반법적 지위를 가지고 있으므로 개인정보보호법 제6조에 따라 개인정보보호법의 개인정보의 국외의 제3자 제공에 관한 규정을 적용할 수 있을 것이다.[83] 즉, 개인정보법 제6조는 개인정보에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다고 정하고 있기 때문에 신용정보법에 개인 신용정보의 국외이전에 관한 명문 규정이 없는 경우 개인정보보호법의 국외 이전에 관한 규정이 보충적으로 적용된다고 보는 것이 타당하다는 것이다.[84][85]

83) 박영우, "글로벌 기업에 대한 개인정보보호 규제효과 제고 및 불법 · 청소년유해정보의 유통금지를 위한 국가간 협력방안 연구", 방통융합정책연구 연구보고서, 방송통신위원회(2014), 50-51면.

84) 최경진, 전게 보고서 "GDPR등 EU와 우리나라 온라인상 개인정보보호 법제 비교 연구", 51-52면.

85) 다만 현재 금융위원회와 금융감독원은 개인신용정보를 해외에서 처리할 목적으로 개인신용정보를 국외로 제공하는 것에 대한 신용정보법상 특별한 규정이 없기 때문에 이는 허용되지 않는다는 해석을 취하고 있다고 한다. 강준모, "우리나라FTA와 전자금융법제", 한국법제연구원(2010. 10), 49면.

또한 신용정보법 제32조 제4항 제8호에서는 '국제협약 등에 따라 외국의 금융감독기구에 금융회사가 가지는 개인신용정보를 제공하는 경우'에는 정보주체의 동의를 받지 않아도 된다고 규정하고 있지만, 이는 '외국의 금융감독기구'에 신용정보거래가 이전되는 경우에 한하므로, 통상적인 금융기관에 우리 국민의 금융거래정보를 제공하는 경우에는 다른 법률이나 법률의 효력을 갖는 조약 등에서 이를 허용하는 등 특별한 사정이 없는 한 원칙에 따라 해당 정보주체의 사전 동의를 얻어야 할 것이다.[86]

한편, '금융회사의 정보처리 업무 위탁에 관한 규정'에서는 금융회사가 고객의 금융거래정보의 처리를 위탁하는 경우(혹은 금융거래정보 처리업무를 위탁받은 자가 다시 제3자에게 재위탁하는 경우), 이 업무를 수탁받은 자가 국외에 소재하는 경우 정보주체에 대한 고지나 동의는 요구되지 않지만 그 위탁계약(혹은 재위탁계약)의 체결을 체결예정일로부터 30영업일 이전에 금융감독원장에게 보고하고(제7조제1항)[87], 이 계약의 내용에는 데이터에 대한 접근통제, 전산사고 등에 따른 이용자 피해에 대한 위·수탁자 간의 책임관계, 수탁자에 대한 감독당국의 감독·검사 수용의무, 수탁회사의 분쟁해결 과정에서의 재판관할 등을 반드시 포함하도록 하여 그 책임관계를 명확히 하도록 규정하고 있다.(제4조제3항) 또한 제5조(특정정보의 보호)에서는 어떠한 경우에라도 개인고객의 고유식별정보는 국외로 이전되지 않아야 한다고 하고 있기도 하다.

---

86) 구태언, "개인정보 국외 이전제도의 현황 및 개선방안 연구", 가천법학 제6권 제1호, 가천대학교 법학연구소(2013), 289면.

87) **금융회사의 정보처리 업무 위탁에 관한 규정 제7조(보고)** ① 금융회사가 제4조제1항에 따라 개인고객의 금융거래정보(금융거래의 내용이 누구의 것인지를 알 수 없는 경우를 제외한다) 처리업무를 위탁하고자 하는 경우로서 업무를 수탁받는 자가 국외에 소재하는 경우에는 그 사실을 업무를 위탁받은 자가 그 위탁받은 업무를 실제로 수행하려는 날의 30영업일 이전에 다음 각 호의 서류를 첨부하여 금융감독원장에게 보고하여야 한다.
1. 위탁계약서(안) 사본
2. 「금융기관의 업무위탁 등에 관한 규정」 제3조의2에 따라 금융기관이 마련하고 준수하여야 할 '업무위수탁 운영기준'
3. 업무위탁 계약이 이 규정 등 관련법령에 위배되지 아니한다는 준법감시인(준법감시인이 없는 경우, 감사 등 이에 준하는 자)의 검토의견 및 관련자료 사본
4. 위탁의 필요성 및 기대효과
5. 위탁에 따른 업무처리절차의 주요 변경내용
6. 정보처리업무 운영에 대한 감독기관의 실질적 감독가능성을 확인할 수 있는 서류
7. 위탁계약 상대방(재위탁 예정시 재위탁계약 상대방 포함)에 관한 사항(상호, 자본금 규모, 소재지, 주된 업종, 개인의 경우 대표자 인적사항 등)
8. 전산사고 및 정보유출 등 발생시 피해자 구제절차

## Ⅳ. 기 타

### 1. 금융실명거래 및 비밀보장에 관한 법률

금융실명법은 별도로 국외이전에 대한 규정을 두고 있지 않지만 제4조에서 “금융회사 등에 종사하는 자는 명의인의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 “거래정보 등”이라 한다)를 타인에게 제공하거나 누설하여서는 아니 되며, 누구든지 금융회사 등에 종사하는 자에게 거래정보 등의 제공을 요구하여서는 아니 된다”고 규정하고, 일정한 경우에만 명의인의 요구나 동의를 받지 않고서도 거래정보 등을 타인에게 제공할 수 있다고 규정(동 조항 단서 각 호)하고 있어 만일 ‘금융회사 등’에서 고객의 거래정보 등을 국외의 제3자에게 이전하려고 한다면 이러한 제4조 제1항의 규정에 따라 명의인으로부터 서면상의 요구나 동의가 필요할 것이다. 명의인의 요구나 동의없이 거래의 정보 또는 자료를 다른 사람에게 제공하는 일정한 경우는 법원의 제출명령 또는 법관이 발부한 영장에 따른 거래정보등의 제공, 조세에 관한 법률에 따라 제출의무가 있는 과세자료 등의 제공과 소관 관서의 장이 상속 · 증여 재산의 확인, 조세탈루의 혐의를 인정할 만한 명백한 자료의 확인, 체납자의 재산조회, 「국세징수법」 제14조제1항 각 호의 어느 하나에 해당하는 사유로 조세에 관한 법률에 따른 질문 · 조사를 위하여 필요로 하는 거래정보등의 제공이나 「국정감사 및 조사에 관한 법률」에 따른 국정조사에 필요한 자료로서 해당 조사위원회의 의결에 따른 금융감독원장 및 예금보험공사사장의 거래정보등의 제공 등 8개의 경우를 규정하고 있으며 이 경우에도 그 사용목적에 필요한 최소한의 범위 내에서 하도록 하고 있다.[88]

88) **금융실명거래 및 비밀보장에 관한 법률 제4조(금융거래의 비밀보장)** ① 금융회사등에 종사하는 자는 명의인(신탁의 경우에는 위탁자 또는 수익자를 말한다)의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 “거래정보등”이라 한다)를 타인에게 제공하거나 누설하여서는 아니 되며, 누구든지 금융회사등에 종사하는 자에게 거래정보등의 제공을 요구하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우로서 그 사용 목적에 필요한 최소한의 범위에서 거래정보등을 제공하거나 그 제공을 요구하는 경우에는 그러하지 아니하다.
1. 법원의 제출명령 또는 법관이 발부한 영장에 따른 거래정보등의 제공
2. 조세에 관한 법률에 따라 제출의무가 있는 과세자료 등의 제공과 소관 관서의 장이 상속 · 증여 재산의 확인, 조세탈루의 혐의를 인정할 만한 명백한 자료의 확인, 체납자의 재산조회, 「국세징수법」 제14조제1항 각 호의 어느 하나에 해당하는 사유로 조세에 관한 법률에 따른 질문 · 조사를 위하여 필요로 하는 거래정

## 2. 클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률에서는 이용자가 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있도록 규정하고 있으며, 정보통신서비스를 이용하는 자는 정보통신서비스 제공자에게 클라우드컴퓨팅서비스 이용 여부와 자신의 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다고 규정하고 있다.

또한 과학기술정보통신부장관은 이용자 또는 정보통신서비스 이용자의 보호를 위하여 필요하다고 인정하는 경우에는 미리 방송통신위원회의 의견을 들어 클라우드컴퓨팅서비

---

보등의 제공

3. 「국정감사 및 조사에 관한 법률」에 따른 국정조사에 필요한 자료로서 해당 조사위원회의 의결에 따른 금융감독원장(「금융위원회의 설치 등에 관한 법률」 제24조에 따른 금융감독원의 원장을 말한다. 이하 같다) 및 예금보험공사사장(「예금자보호법」 제3조에 따른 예금보험공사의 사장을 말한다. 이하 같다)의 거래정보등의 제공
4. 금융위원회(증권시장 · 파생상품시장의 불공정거래조사의 경우에는 증권선물위원회를 말한다. 이하 이 조에서 같다), 금융감독원장 및 예금보험공사사장이 금융회사등에 대한 감독 · 검사를 위하여 필요로 하는 거래정보등의 제공으로서 다음 각 목의 어느 하나에 해당하는 경우와 제3호에 따라 해당 조사위원회에 제공하기 위한 경우
   가. 내부자거래 및 불공정거래행위 등의 조사에 필요한 경우
   나. 고객예금 횡령, 무자원(無資源) 입금 기표(記票) 후 현금 인출 등 금융사고의 적발에 필요한 경우
   다. 구속성예금 수입(受入), 자기앞수표 선발행(先發行) 등 불건전 금융거래행위의 조사에 필요한 경우
   라. 금융실명거래 위반, 장부 외 거래, 출자자 대출, 동일인 한도 초과 등 법령 위반행위의 조사에 필요한 경우
   마. 「예금자보호법」에 따른 예금보험업무 및 「금융산업의 구조개선에 관한 법률」에 따라 예금보험공사사장이 예금자표(預金者表)의 작성업무를 수행하기 위하여 필요한 경우
5. 동일한 금융회사등의 내부 또는 금융회사등 상호간에 업무상 필요한 거래정보등의 제공
6. 금융위원회 및 금융감독원장이 그에 상응하는 업무를 수행하는 외국 금융감독기관(국제금융감독기구를 포함한다. 이하 같다)과 다음 각 목의 사항에 대한 업무협조를 위하여 필요로 하는 거래정보등의 제공
   가. 금융회사등 및 금융회사등의 해외지점 · 현지법인 등에 대한 감독 · 검사
   나. 「자본시장과 금융투자업에 관한 법률」 제437조에 따른 정보교환 및 조사 등의 협조
7. 「자본시장과 금융투자업에 관한 법률」에 따라 거래소허가를 받은 거래소(이하 "거래소"라 한다)가 다음 각 목의 경우에 필요로 하는 투자매매업자 · 투자중개업자가 보유한 거래정보등의 제공
   가. 「자본시장과 금융투자업에 관한 법률」 제404조에 따른 이상거래(異常去來)의 심리 또는 회원의 감리를 수행하는 경우
   나. 이상거래의 심리 또는 회원의 감리와 관련하여 거래소에 상응하는 업무를 수행하는 외국거래소 등과 협조하기 위한 경우. 다만, 금융위원회의 사전 승인을 받은 경우로 한정한다.
8. 그 밖에 법률에 따라 불특정 다수인에게 의무적으로 공개하여야 하는 것으로서 해당 법률에 따른 거래정보등의 제공

스 제공자 또는 정보통신서비스 제공자에게 이용자의 정보가 저장되는 국가의 명칭을 공개하도록 권고할 수 있다.[89]

## 제2절 우리나라가 당사자인 자유무역협정(FTA)

앞서 살펴본 바와 같이 우리나라는 해외에서 우리 국민의 개인정보가 안전하게 유통될 수 있도록 개인정보 보호법, 정보통신망법 등을 통하여 개인정보를 국외이전하기 위해서 비교적 엄격한 요건을 준수하도록 하고 있다. 그러나 우리나라는 무역을 증진시키기 위하여 미국, EU 등 여러 나라와 자유무역협정을 체결하면서 국경 간 개인정보의 이전을 용이하게 하기 위한 조항을 두고 있다. 정보통신기술의 발달에 따라 국가 간의 물자나 서비스가 이동하는 무역에서 전자거래나 서비스가 많은 부분을 차지하고 있고 이러한 국제거래에서 개인정보를 포함, 데이터가 국경을 넘어서 이동하는 것 또한 불가피한 상황인데 이를 과도하게 규제하게 된다면 이는 곧 그에 기반한 국제 무역을 제한하게 되기 때문이다.

### Ⅰ. 한-미 자유무역협정

한-미 자유무역협정(FTA)을 보면 제13장 '금융서비스'의 '13-나 구체적 약속' 제2절(정보의 이전),[90]에서 "각 당사국은 다른 쪽 당사국의 금융기관이 그 기관의 일상적인 영업

89) **클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 제26조(이용자 보호 등을 위한 정보 공개)** ① 이용자는 클라우드컴퓨팅서비스 제공자에게 이용자 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.
② 정보통신서비스(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제2호에 따른 정보통신서비스를 말한다. 이하 제3항에서 같다)를 이용하는 자는 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제3호에 따른 정보통신서비스 제공자를 말한다. 이하 제3항에서 같다)에게 클라우드컴퓨팅서비스 이용 여부와 자신의 정보가 저장되는 국가의 명칭을 알려 줄 것을 요구할 수 있다.
③ 과학기술정보통신부장관은 이용자 또는 정보통신서비스 이용자의 보호를 위하여 필요하다고 인정하는 경우에는 클라우드컴퓨팅서비스 제공자 또는 정보통신서비스 제공자에게 제1항 및 제2항에 따른 정보를 공개하도록 권고할 수 있다.
④ 과학기술정보통신부장관이 제3항에 따라 정보를 공개하도록 권고하려는 경우에는 미리 방송통신위원회의 의견을 들어야 한다.

90) **SECTION B: TRANSFER OF INFORMATION** Each Party shall allow a financial institution of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such

과정에서 데이터 처리가 요구되는 경우 그러한 처리를 위하여 자국 영역 안과 밖으로 정보를 전자적 또는 그 밖의 형태로 이전하는 것을 허용한다. 대한민국은 이 협정 발효일 후 2년 내에 이 약속에 효력을 부여한다.”라고 규정하고 있어 금융거래에 관한 개인정보가 국외이전의 대상에 포함된다는 것을 명확히 밝히고 있고, 나아가 제3절(기능의 수행)의 제1항에서는 “양 당사국은 당사국 영역 내의 금융기관이 그 당사국의 영역 안 또는 밖에 소재한 그 기관의 본점 또는 계열사에서 일정 기능을 수행하도록 허용하는 것이 유익함을 인정한다. 실행가능한 한도에서 각 당사국은 그러한 본점 또는 계열사가 이 기능을 수행하는 것을 허용하여야 할 것이다.”[91]라고 규정하면서 그 기능에는 ‘데이터 처리, 프로그래밍 및 시스템 발과 같은 기술 관련 기능’[92]등이 있다고 설명하면서 여기서 말하는 데이터 처리란 ‘당사국이 부속서 13-나 제2절에 따라 자국 영역 밖으로 정보의 이전을 허용할 의무를 지는 한도에서, 그 당사국은 또한 이전 후 그 정보의 데이터처리를 허용한다’라고 되어 있다.

또한 위 부속서 외에 이 협정의 추진 당시에 당사국 사이에 오고갔던 ‘부속서한’에 따르면 “양 당사국은 금융기관에 의한 국경 간 정보이전의 중요성을 인정하며, 미합중국은 부속서 13-가 제6항 나호 및 부속서 13-나 제2절에서 그러한 기관이 그러한 정보를 이전하도록 허용할 자국 규제제도의 개정을 시행하겠다는 대한민국의 약속을 환영한다. 대한민국은 소비자의 민감 정보의 보호 그 민감정보의 무단 재사용의 금지 그러한 정보의 취급에 관한 금융기관의 기록에 접근할 수 있는 금융감독기관의 권한 기술설비의 위치에 대한 요건과 같은 분야에 대하여, 그러한 개정이 미합중국의 접근방법과 유사한 접근방법을 택하는 결과가 될 것이라는 의사를 표현하였다.”[93]라고 되어 있다.[94] 이에 따라 금융

processing is required in the institution’s ordinary course of business. Korea shall give effect to this commitment no later than two years after the date this Agreement enters into force.

91) **SECTION C: PERFORMANCE OF FUNCTIONS** The Parties recognize the benefits of allowing a financial institution in a Party's territory to perform certain functions at its head office or affiliates located inside or outside the Party’s territory. To the extent practicable, each Party should allow such an office or affiliate to perform these functions.

92) technology-related functions, such as data processing, programming, and system development;

93) The Parties recognize the importance of the cross-border transfer of information by financial institutions, and the United States welcomes Korea’s commitment in paragraph 6(b) of Annex 13-A and Section B of Annex

위원회는 2015년 '금융회사의 정보처리 및 전산설미 위탁에 관한 규정'을 개정하여 금융거래정보가 국외이전되는 것을 명시적으로 허용하고 있는데, 이러한 개정은 금융회사가 콜센터나 총무, 회계 인사업무 등의 후선지원업무, 자산운용부문, IT운영부문 등을 외국기업에게 위탁, 처리할 수 있게 하였다. 그러나 이렇듯 우리나라가 우리나라의 금융거래정보 국외이전제도를 한·미 FTA에 따라 미국의 법제도에 맞춰 개정하게 되는 경우, EU의 지침은 국외이전된 개인정보의 재이전을 제한하고 있어 유럽의 금융회사들의 금융정보는 국내로 들여올 수 없는 결과를 초래할 수 있다고 한다.[95]

한편 15장 전자상거래에서는 전자상거래 분야에서 각 당사국이 무역을 원활히 하기 위하여 정보의 자유로운 흐름의 중요성을 인정하고 개인정보 보호의 중요성을 인정하면서, 국경 간 전자 정보 흐름에 불필요한 장벽을 부과하거나 유지하는 것을 자제하도록 노력해야 한다고 하기도 하였다.[96]

## Ⅱ. 한-EU 자유무역협정

한-EU FTA도 금융서비스 공급자에 의한 정보의 국경 간 이전을 허용한다고 규정하고 있다. 즉 한-EU 자유무역협정 제7.43조(자료 처리)는 '이 협정 발효 후 2년 이내에 그리고 어떠한 경우에도 다른 경제통합협정으로부터 발생하는 유사한 약속의 발효일 이내에 (가)각 당사자는 자신의 영역 내에 설립된 다른 쪽 당사자의 금융서비스 공급자가 그러한

13-B to undertake modifications to its regulatory regime that will permit those institutions to transfer such information. Korea has expressed its intent that these modifications will result in its adoption of approaches that are similar to those of the United States with respect to such areas as the protection of sensitive information of consumers, prohibitions on unauthorized reuse of the sensitive information, the ability of financial regulators to have access to records of financial institutions relating to the handling of such information, and requirements for the location of technology facilities.

94) 구태언, 전게 "개인정보 국외 이전제도의 현황 및 개선방안 연구", 304-305면.

95) 이창범, 전게 "한국의 개인정보 국외이전 법제 현황과 개정방향", 380면.

96) **ARTICLE 15.8: CROSS-BORDER INFORMATION FLOWS** Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.

금융서비스 공급자의 일상적인 영업과정에서 자료 처리가 요구되는 경우, 그러한 처리를 위해 자신의 영역 안과 밖으로 정보를 전자적 또는 그 밖의 형태로 이전하는 것을 허용한다. 그리고 (나)각 당사자는 개인의 기본권 및 자유를 보호하기 위한 자신의 약속을 재확인하면서, 특히 개인자료의 이전에 대하여 사생활의 보호를 위한 충분한 보호장치를 채택한다.'[97]라고 하여 한-미 FTA와는 달리 금융거래정보의 국외이전에 따른 프라이버시 보호를 위한 충분한 장치의 마련에 더 무게를 두고 있다. 또한 동 부속서 7-라에서는 정보이전의 허용방안을 마련할 때에 ① 소비자의 민감정보의 보호, ② 그 민감정보의 무단재사용 금지, ③ 그러한 정보의 취급에 관한 금융서비스 공급자의 기록에 접근할 수 있는 금융규제기관의 능력, ④ 기술설비의 위치에 대한 요건과 같은 분야를 다루면서 금융정보의 국경 간 이전을 허용하는 접근방법을 채택하기로 하고 있다.[98]

이에 따라 한-EU 자유무역협정은 세계인권선언, 컴퓨터화된 개인정보파일의 규제를 위한 UN지침(1990년 12월 14일 국제연합 총회 결의 45/95로 채택), 사생활 보호 및 개인정보의 국경간 이동에 관한 OECD 지침(1980년 9월 23일 경제협력개발기구 이사회 채택) 등에서 규정하고 있는 개인의 기본권 및 자유를 보호하기 위한 약속을 지킬 것을 재확인하는 한편, 개인정보 국외 이전시 사생활 보호를 위한 충분한 보호조치를 채택할 것을 요구하는 등(제7.43조 나) 전반적으로 금융거래정보의 자유로운 이전보다는 보호를 중요

97) **ARTICLE 7.43: DATA PROCESSING** No later than two years after the entry into force of this Agreement, and in no case later than the effective date of similar commitments stemming from other economic integration agreements:
(a) each Party shall permit a financial service supplier of the other Party established in its territory to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier; and
(b) each Party, reaffirming its commitment38 to protect fundamental rights and freedom of individuals, shall adopt adequate safeguards to the protection of privacy, in particular with regard to the transfer of personal data.

98) **ANNEX 7-D, THE ADDITIONAL COMMITMENT ON FINANCIAL SERVICES 1. Transfer of information** The Parties recognise the importance of the cross-border transfer of information by financial service suppliers. Korea has expressed its intent to undertake modification to its regulatory regime that will result in its adoption of approaches that will permit the transfer of financial information across borders while addressing such areas as the protection of sensitive information of consumers, prohibitions on unauthorised reuse of the sensitive information, the ability of financial regulators to have access to records of financial service suppliers relating to the handling of such information, and requirements for the location of technology facilities

시하고 있다고 할 수 있는데, EU 시민의 개인정보가 한국을 거쳐 다른 나라로 재이전되지 않도록 안전조치를 취하라는 의미인 것이다.[99]

## 제3절 현행 법령 분석

### Ⅰ. 법령 간 정합성 문제

앞서 살펴본 바와 같이 우리나라는 개인정보보호법이라는 일반법을 마련하여 두고 개별법으로 정보통신망법, 신용정보법 등을 두고 있어 법령간의 충돌이나 형평성의 문제가 제기될 수 있다.

먼저 예를 들면 개인정보보호법은 국외의 제3자 제공에 대하여 규정하고 있고 정보통신망법은 제3자제공, 위탁, 인수나 합병 등의 원인에 관계없이 국외이전에 관하여 규정하고 있는데, 어떤 법이 적용되는가에 따라 정보주체의 동의를 필요로 하는지의 여부가 달라지기 때문에 당사자들에게 중요한 문제라고 할 수 있음에도, 구체적인 어떤 개인정보 국외이전 사례에 어느 법이 배타적으로 적용되는지 아니면 중첩적으로 적용되는지를 확정하는 것이 간단하지 않다. 만일 신용정보법의 적용을 받는 신용정보회사나 보험회사 등이 개인신용정보를 '국외의 제3자'에게 '제공'하는 경우에는 신용정보법에 특별한 규정이 있는 경우에 해당하기 때문에 개인정보보호법 제6조에 따라 개인정보법이 아니라 신용정보법이 적용되어 신용정보회사나 보험회사 등은 그 정보주체에게 사전 동의를 받아 개인신용정보를 국외로 이전할 수 있다.

그런데 신용정보회사가 동시에 정보통신서비스제공자인 경우에는 정보통신망법이 적용되기 때문에 신용정보회사는 정보통신망법의 규정에 따라 국외의 제3자에게 제공하는 경우 외에도 위탁을 하거나 합병 등을 하는 경우에도 정보주체의 동의를 얻어야 한다.

99) 이창범, 전게 "한국의 개인정보 국외이전 법제 현황과 개정방향", 380-381면.

또한 정보통신서비스제공자는 개인정보를 국외의 제3자에게 제공하는 경우뿐만 아니라 위탁, 영업양도・양수 등에 있어서 개인정보의 '국외 이전'이 수반될 경우에 정보통신망법 제63조가 정하는 바에 따라 고지를 하고 사전 동의를 받아야 한다.[100]

마지막으로 신용정보법이나 정보통신망법의 규율 대상이 아닌 개인정보 보호법상 개인정보처리자는 개인정보 보호법에 따라 국외의 제3자에게 제공하는 경우에 한하여 동의를 받으면 된다.[101]

이처럼 단어나 요건 하나하나마다 그 적용범위나 내용이 달라지는데 사례마다 어떤 법이 적용되는지 판단하는데에 어려움이 있기 때문에 이를 통일할 필요성이 있다.

## Ⅱ. 실무적 측면의 문제점

개인정보를 국외이전하기위해서 우리 법은 정보주체의 동의를 전제로 하고 있다. 그런데 만일 어떤 사업자가 국내에서 수집한 고객의 개인정보를 해외의 제3자에 업무를 위탁하여 국외 이전을 하려고 한다면 그 사업자는 이전하려고 하는 고객에 일일이 동의를 받아야 하며, 게다가 이용자의 동의 외에는 다른 어떤 대안(예를 들면 세이프하버 원칙, 표준계약서 등)을 전혀 인정하고 있지 않기 때문에 이는 사업자에 지나치게 엄격하다는 목소리가 높다. 게다가 이용자는 국내의 어떤 서비스를 이용하고자 할 때 자신의 정보가 국외로 이전될 수 있다는 것에 대하여 깊게 생각하지 않고 서비스를 이용하기 위하여 무심히 동의할 가능성이 높아 이러한 동의규정이 반드시 이용자의 보호에 가장 적합한 방식이라고 보기도 어렵다.

또한 이렇게 국외이전에 대하여 이용자의 동의만 얻게 되면 오히려 이러한 이용자의 개인정보가 비교적 정보보호수준이 낮은 국가에 국외이전 된다고 하더라도 사업자는 면책을 받을 수 있다고 여겨 악용될 가능성도 있다. 따라서 국외이전 되는 대상 국가의 정

100) 구태언, 전게 "개인정보 국외 이전제도의 현황 및 개선방안 연구", 292면.
101) 구태언, 앞의 논문, 291-292면.

보보호 수준이 어느 정도인지 국가기관이 판단하여 이에 따라 차등적으로 동의를 받게 하는 등의 방안이 필요할 것으로 보인다.[102)]

## Ⅲ. 효율적 국외이전체계의 필요성

EU는 유럽연합 회원국 국민의 개인정보를 유럽연합 역외 지역으로 이동하는 경우에 원칙적으로 정보주체의 동의를 필요로 하지 않고, 유럽연합의 개인정보 보호 수준과 동일한 개인정보 보호 수준을 갖춘 국가나 국제기구로만 유럽연합 회원국 국민의 개인정보 이동을 허용하는 규정을 두고 있다.

예를 들어 EU 회원국 국민의 개인정보를 제3국으로 이전하려고 할 때 제3국이 국가 단위로 개인정보 보호 수준에 대하여 EU의 적합성 평가받아야 하고, 이를 통과하지 못한 경우 해당국의 기업이나 조직이 개별적으로 EU가 요구하는 적절한 수준의 보호조치를 마련하여야 하도록 하고 있으며 이렇게 이전된 개인정보가 또다른 국가로 재이전 되는 것을 제한함으로써 자국민의 개인정보를 보호하고 있다. 이러한 규정에 따라, 유럽연합 회원국의 개인정보 보호 기준보다 낮은 보호 기준을 가진 국가이거나 이러한 기준과 상이한 기준을 가진 국가로는 유럽연합 회원국의 개인정보가 이동될 수 없도록 하고 있기 때문이다.[103)]

또한 미국와 EU의 새로운 개인정보 이전 협약인 Privacy Shield Agreement에서는 기존의 세이프하버 조약보다 개인정보보호 준수 의무를 강화하여 유럽에서 개인정보를 이전하고자 하는 미국 기업은 유럽의 데이터 주체의 권리 보장 등에 대한 보다 엄격한 주의의무를 준수하도록 하고,[104)][105)] 요건을 충족하지 못하는 기업들은 개인정보 이전에 필요

102) 최경진, “개인정보 국외이전 법제 정비방안”, 연구보고서, 한국인터넷진흥원(2012), 61면.
103) 노현숙, “EU 개인정보 국외 이동 규정의 유용성”, 법학논총 제36집, 숭실대학교 법학연구소(2016), 13면.
104) 세부 내용으로서, 자세한 내용이 담긴 통지 의무, 데이터 보유 유지 제한, 접근권 보장, 3자 전송의 엄격한 조건, 데이터 무결성 확보, 목적 제한, 그리고 보다 강화된 보안 요건 등이다.
105) 프라이버시 쉴드는 2015년 10월에 EU사법재판소(Court of Justice of the European Union)가 기존의 세이프하버 방식이 적절성 평가 기준에 비추어 볼 때 EU시민의 개인정보를 충분하게 보호하지 못한다고 하여 세이프

한 법적 지위를 잃게 되며, 이러한 협약 하에서 자신의 권리를 침해당한 개인은 누구나 여러 종류의 구제수단을 이용할 수 있게 된다.[106]

일본 역시 일본과 해외 사업자가 자국민의 개인정보를 수집한 경우에는 일본의 개인정보보호법을 적용받으며, 일본과 동등한 개인정보 수준을 갖춘 국가에 대하여는 사전 동의 없는 국외 이전을 허용하는 제도를 가지고 있다.

**<표 3-1> 주요국의 개인정보 국외이전 제도**

| 국가 | 법률 및 조항 | 내용 |
|---|---|---|
| EU | GDPR 제44조, 제45조 적합성평가 | EU 역외국가가 EU의 개인정보 보호지침에서 요구하는 수준으로 개인정보를 보호하고 있는지를 평가하는 제도 |
| | GDPR 제47조 구속력 있는 기업 규칙 | EU 역내에서 사업 활동을 하는 기업그룹이 그룹 내부의 정보교류 시 EU 개인정보보호원칙을 준수할 것임을 확약하고 정보주체의 각종 권리구제수단을 정해놓은 행동강령 |
| | GDPR 제46조 표준정보보호 조항 | 표준계약조항에 따라 개인정보를 이전하고자 하는 경우 감독당국의 별도 허가가 필요하지 않음. 다만, 유효한 표준계약이 되려면 집행위원회가 채택한 것이거나, 감독당국이 채택하고 집행위원회가 승인한 것이어야 함 |
| | GDPR 제45조 2항 개인정보 재이전 | 제45조 2항 (a)에서는 제3국이나 국제조직의 보호수준 적합성을 평가 시 해당 국가나 국제조직에서 준수되는 개인정보의 다른 제3국이나 국제조직으로의 계속적인 이전을 위한 규정과 해당 규정 관 |

하버의 무효를 판결(일명 Schrems 판결, Case C-362/14)함에 따라 새롭게 마련된 것이다.

106) 이러한 구제 수단으로서 개인은 먼저 ①해당 기업에 직접적으로 불만을 제기하여 해당 기업이 이를 45일 안에 해결할 수 있다. 또한 ②EU의 개인정보감독기구에 직접 불만을 제기하는 경우 감독기구가 미 연방정부 거래위원회에 이러한 내용을 전달하여 연방거래위원회로 하여금 개인의 불만을 처리하도록 하며, 만일 연방거래위원회가 이를 처리하지 않을 경우 무료로 분쟁조정을 위한 대체수단을 제공하도록 하고 있다. ③ 만일 미 국가정보기관에 의한 개인정보 침해가 발생할 경우, 미국무부내에 이를 해결할 수 있는 새로운 담당부서로서 옴부즈만 시스템을 갖추도록 하고, 이 부서는 정보기관과 독립적으로 운영, 유럽연합 개인정보감독기구가 제기한 이슈에 대해 검토하며, 미 상무부의 고위 관리가 프라이버시 쉴드 옴부즈만 부서를 관장토록 한다. 윤재석, “유럽연합과 미국의 개인정보 이전 협약(프라이버시 쉴드)과 국내 정책 방향”, 정보보호학회 논문지 제26권 제5호, 한국정보보호학회(2016), 1273면.

| 국가 | 법률 및 조항 | 내용 |
|---|---|---|
| | 제한 | 련 입법, 그리고 보안조치의 실행 등에 대하여 평가하도록 함 |
| 미국 | Privacy Shield Agreement | EU-미국 간 개인정보의 국외이전 관련, 기존 세이프 하버(Safe Harbor) 협약에 비하여 개인정보 보호 준수 부문을 강화 |
| 일본 | 개인정보보호법 국외이전조항 | 자국민의 개인정보를 수집한 국외의 사업자들에게 일본 개인정보 보호법을 적용하도록 하고 있으며, 일본과 동등한 개인정보 보호 수준 인정 국가에 대하여서는 사전 동의 없는 국외 이전을 허용 |
| 국내 | 개인정보보호법 제14조 | 1항 - 정부는 국제적 환경에서의 개인정보 보호 수준을 향상시키기 위하여 필요한 시책을 마련하여야 함<br>2항 - 개인정보 국외 이전으로 인해 정보주체의 권리가 침해되지 않도록 정부가 시책을 마련하여야 함 |
| | 개인정보보호법 제17조 | 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 경우 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로는 개인정보의 국외 이전에 관한 계약을 체결하지 못하도록 규정 |

출처 : 김인석, 국제적 상호운용성 강화 및 지능정보화 시대에 부응한 개인정보보호 발전 방안 연구, 개인정보보호위원회 정책연구용역 연구보고서, 개인정보보호위원회, 2016

그렇지만 국내 개인정보보호법은 개인정보의 국외이전에 대하여 정보주체의 동의를 받도록 규정하고 있을 뿐 이러한 EU의 구속력 있는 기업 규칙이나 표준계약조항, 프라이버시 쉴드와 같은 조항은 포함하고 있지 않다.

다시 말하면 EU의 이러한 조항들은 제3국이 국가 단위로 EU의 적합성 평가를 통과하지 못한 경우 해당국의 기업이나 조직이 개별적으로 EU가 요구하는 적절한 수준의 보호조치를 마련하도록 하여 개인정보의 국외이전을 가능토록 함으로써 증가하는 국가 간 교역에 따라 피할 수 없는 국가 간의 개인정보 이전에 대하여 EU 자국민의 개인정보를 최대한으로 보호하고 한편으로는 교역의 활성화도 이루어지도록 하고 있고, 또한 EU 적합성 평가 기준에서 국외로 이전된 개인정보의 재이전을 제한하는 규정으로 국외로 이전된 개인정보에 대한 사후적 관리조치를 하도록 하고 있는데 우리나라는 아직 이러한 부분에서 제도적 미비가 존재하는 것이다. 무역의 활성화를 위하여 국외 개인정보법에 맞추기 위하여 EU 적합성 평가 신청 등의 노력은 하고 있으나 우리의 개인정보를 보호하기 위한 국외 이전

시스템은 보완이 시급한 상황이다. 따라서 유럽의 적합성 평가나 일본의 동등한 개인정보 보호 수준 인정 국가에 대한 사전 없는 국외 이전 허용에 관한 조항 등과 같이 우리나라도 다른 나라와의 개인정보 보호제도와 균형을 맞출 수 있는 보호장치를 마련함으로써 데이터 이전을 전제로 한 무역의 활성화를 꾀할 뿐 아니라 자국민의 데이터의 안전한 국외 이전 및 활용을 도모할 수 있는 제도의 도입을 검토할 필요가 있다.[107]

107) 김인석, "국제적 상호운용성 강화 및 지능정보화 시대에 부응한 개인정보보호 발전 방안 연구", 개인정보보호위원회 정책연구용역 연구보고서, 개인정보보호위원회(2016), 89-93면.

korea
legislation
research
institute

# 제4장
# 해외에서의 우리 국민의 개인정보의 효과적인 보호를 위한 법제도 개선 방안 연구

제1절 개인정보 이전에 관한 효과적인 규율체계 정립방안
제2절 국제적인 공조체계 및 상호주의적 보호체계 구축

# 제4장 해외에서의 우리 국민의 개인정보의 효과적인 보호를 위한 법제도 개선 방안 연구

## 제1절 개인정보 이전에 관한 효과적인 규율체계 정립방안

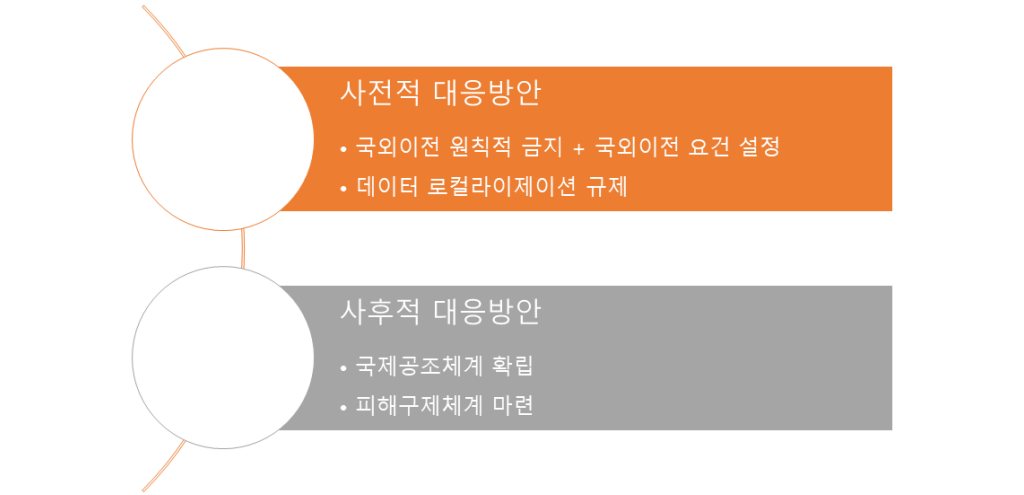
### Ⅰ. 해외에서의 우리 국민의 개인정보보호의 필요성

사물인터넷으로 전세계가 연결되고 정보처리가 고도화됨에 따라 네트워크를 통하여 해외 사업자나 정부, 단체 등이 우리나라 국민의 개인정보를 광범위하게 수집하고 처리하는 경우가 증가하는 것은 불가피한 방향이다. 더욱이 우리나라는 국제적인 무역을 국가발전의 원동력으로 삼고 있는 나라이기 때문에 4차 산업혁명 시대에 국가간의 개인정보의 이동을 완전히 막을 수도 없다. 미래 지능정보화 사회에서 데이터나 개인정보는 가장 핵심적인 원료로서 그 사회적·경제적 가치는 측량하기 어려울 정도로 클 것으로 예상된다. 때문에 개인정보의 이전을 막는 것은 '디지털 쇄국정책'이라고 부를 수 있을 만큼 우리 경제발전에 도움이 되지 못한다는 평가가 가능할 것이다. 그렇지만 국민의 개인정보는 일단 국외로 이전되어 통제 불능의 상태에서 처리가 계속된다면, 지속적으로 국민들에게 정신적·경제적 피해를 야기할 가능성도 배제할 수 없다. 따라서 우리 국민의 기본적 자유나 권리와 직결될 수도 있는 개인정보가 해외로 나가는 경우에 적절한 안전조치를 하거나 사후적으로라도 해당 개인정보에 대한 통제권을 잃지 않게 만드는 제도적 장치가 필요하며, 나아가 국민의 개인정보가 유출되거나 침해되는 경우에도 효과적으로 피해확산을 방지하고 피해를 구제할 수 있는 제도적 장치를 만드는 것도 매우 중요하다. 정보 유통의 시대에 우리 국민의 개인정보가 해외로 나가기 전에 일정한 안전망을 만드는 방안과 해외로 이전된 이후에 피해 구제를 위한 체계를 만드는 방안 등에 대한 논의가 필요하다.

## Ⅱ. 해외에서의 개인정보 보호방안

해외로 이전된 우리 국민의 개인정보를 보호하기 위한 방안은 개인정보가 해외로 이전되기 전의 대응방안과 해외로 이전된 후의 대응방안으로 구분해서 검토해볼 수 있다. 해외로 이전되기 전후의 대응방안은 완전히 분리된 별개의 것은 아니고 대응방안을 어떻게 마련하는가에 따라서 국외이전 전후가 모두 연계되거나 어느 하나에 보다 더 초점이 맞춰진 경우도 있을 것이다.

[해외로 이전된 개인정보 보호방안] - ⓒ최경진




국민의 개인정보가 해외로 이전되기 전의 대응방안으로는 (1) 국외이전을 원칙적으로 금지하고 예외적으로 허용하되, 국외이전의 요건을 엄격히 설정하는 방안, (2) 외국 사업자나 정부 등이 우리 국민의 개인정보를 처리하기 위해서는 국내에 서버나 사무소를 두고 처리하게 하는 방안 등이 고려될 수 있다. 국외이전을 원칙적으로 금지하고 예외적으로 허용하되, 국외이전의 요건을 엄격히 설정하는 방안을 추진하는 경우에도 예외적 허용범위와 국외이전의 요건을 어떻게 설정하는가에 따라 다양한 방안이 도출될 수도 있다. 국외이전 요건의 경우에도 국외이전을 하는 자 또는 국외이전을 받는 자에게 일정한 안

전조치를 취하는 경우에 이전을 허용하는 방안이나 국외이전에 따른 개인정보보호 방안을 마련토록 강제하는 방안 등이 고려될 수 있다. 이렇게 국외이전을 제한하는 정책을 추진하는 경우에 실제 추진하기 위한 법적 근거나 강제력 수반 여부에 따라 구체적인 추진 방안을 달라질 수 있다. 즉, 가장 약한 정책 추진 방안은 (1) 개인정보의 국외이전 시 요건 설정이나 보호조치 요구 등을 단순한 지침이나 가이드라인에 의하여 추진하거나 국외이전 하는 자의 자율규제에 맡기는 방안이다. 그러나 이러한 방안은 그 실효성이 떨어지고 실제 준수 여부도 확보되기 어렵다는 문제가 있다. 이 보다 강한 것은 결국 (2) 법률에 개인정보의 국외이전에 대한 명확한 법적 근거를 두고, 원칙적인 금지와 예외적인 허용 요건을 명시하는 것이다. 우리나라의 개인정보 보호법이나 정보통신망법이 사실상 이러한 한 방식을 채택하고 있고, EU GDPR도 유사한 방식으로 개인정보의 국외이전을 규율하고 있다. 국내 강제력이 있는 법률에 따른 국외이전의 규율방식은 자율규제보다 훨씬 효과적이고 실행력이 높다는 장점이 있지만, 자칫 개인정보의 국가간 이동을 막게 되어 국제 무역 장벽으로 작용할 수 있다는 문제가 지적될 수 있다. 한편, 우리나라의 국제적인 위상이나 국력에 따라서 실제 해외 사업자나 정부 등이 우리 법제를 준수할 것인지의 여부가 결정되거나 상당한 영향력을 받을 수 있고, 결국 강대국들의 경우에 우리나라의 법제를 인정하지 않을 가능성이 있다는 점은 현실적으로 부인하기 어렵다. 이러한 국제적인 효력 문제를 뛰어 넘기 위해서는 결국 (3) 우리 국민의 개인정보를 보호하기 위한 다자간 국제협약을 체결하거나 특정 국가와의 양자협약의 체결을 추진하는 방안이 현실적이다. 그러나 자유무역협정체결이 쉽지 않은 것과 마찬가지로 국가간 개인정보의 이동에 관한 국제협정을 추진한다는 것 또한 쉽지 않다는 단점이 있다.


한편, 사후적으로 국민의 개인정보가 해외로 이전된 이후의 개인정보 보호수단으로는 사후적으로 개인정보가 침해된 이후 피해확산을 방지하기 위한 국가간의 공조체계를 만들거나 사후적인 피해구제를 효과적으로 해줄 수 있는 협력체계를 마련하는 방안 등이 고려될 수 있다. 각각의 대응방안에 대한 상세한 논의는 이하에서 보다 구체적으로 살펴보겠다.

## Ⅲ. 국외이전시 자율규제 유도

우리 국민의 개인정보가 국외로 이전된 경우에 해외 사업자나 정부 등에 의한 자율규제(self regulation)를 활성화할 수 있도록 우리 정부가 '글로벌 환경에서의 개인정보보호 가이드라인' 등을 마련하고 이를 준수할 것을 권고 또는 홍보하는 고려해볼 수 있다. 또한 비록 우리법을 그대로 준수하지는 못한다고 하더라도 국제적으로 통용되거나 인정될 수 있는 다양한 인증을 획득하도록 유도하는 것도 하나의 방안이 될 수 있다. 아울러 우리 법제에 대한 적합성 혹은 준수 자율평가를 유도하고, 그 결과를 국외이전 전에 공표하도록 권고하거나 유도함으로써 법에 대한 준수(Compliance)를 촉진할 필요가 있다. EU GDPR이나[108] 미국 등 글로벌 기업들이 개인정보의 국가간 이전에서 많이 활용하는 구

108) GDPR Article 47.

속력 있는 기업 규칙(Binding Corporate Rules)이나 표준계약서의 활용도 적극 유도할 필요가 있다. 그런데, 이러한 자율규제의 유도는 기업이 자발적으로 참여한다면 상당한 효과를 볼 수 있겠지만, 그 전제가 되는 기업의 자발적 참여가 없이는 실효성이 적다는 문제가 있다. 또한 자율규제와 같은 접근 방식은 해외 정부나 공공기관과 같이 공적 기관에게 기대하기는 어려운 점도 한계이다.

## Ⅳ. 데이터 국지화 입법 방안 검토

데이터 국지화(data localization)는 데이터 주권(data sovereignty) 개념에 기초하여 자국민의 개인정보를 수집, 이용, 보관 등 처리하는 경우에 그 처리를 자국 내에서 이루어지도록 법으로 강제하는 경우를 의미한다. 데이터 국지화를 강제하는 법을 제정하는 경우에 자국민의 개인정보가 해외로 이전되는 것을 엄격히 차단하게 되기 때문에 자국민의 개인정보를 보호하는 데에는 비교적 효과적이다. 반면, 데이터 국지화 법제는 국제적인 무역을 증진하는 데에는 역행하는 법제가 될 수 있다.[109] 특히 우리나라와 같이 국제무역을 중요하게 다루는 국가일수록 데이터 국지화는 미래 지능정보사회에서 경제에 악영향을 줄 가능성도 배제할 수 없다. 그럼에도 호주의 건강기록, 캐나다 노바 스코샤 주나 브리티시 컬럼비아 주의 공공기관 서비스의 개인정보, 중국, 독일의 통신 메타데이터, 인도네시아의 공공서비스, 카자흐스탄의 국가도메인 운영 서버, 나이지리아의 모든 정부 데이터, 러시아의 모든 개인정보, 우리나라의 지도 데이터, 베트남의 서비스 제공자 이용 데이터 등의 사례에서와 같이 내국법으로 데이터 국지화를 강제하는 경우를 찾아볼 수 있다. 더욱이 대부분의 국가는 국가안보(national security)와 관련한 정보의 국외 이전을 제한한다. 개인정보가 국민의 프라이버시나 본질적인 자유와 권리, 국가안보 등과 같이 매우 중요한 국익과 관련된 경우에는 데이터 국지화와 같은 강력한 수단을 동원할 필요가 있겠지만,

109) 이러한 점을 고려하여 환태평양경제동반자협정(Trans-Pacific Partnership)의 협상 과정에서 참가국 사이에서의 데이터 국지화를 금지하는 규정을 포함하는 것이 논의되었었다. Shaun Waterman, “Trans-Pacific Partnership will ban data localization laws”, fedscoop in OCt 5, 2015. <https://www.fedscoop.com/tpp-will-ban-data-localization -laws/> (2018.10.31. 최종방문).

개인정보는 그 스펙트럼이 매우 다양하여 단순히 아주 간단한 서비스를 위한 간단한 정보로부터 국익과 직결되는 매우 중요한 개인정보에 이르기까지 매우 넓은 범위에 걸쳐있기 때문에 일반적 측면에서 데이터 국지화를 강제하는 입법을 제정하는 것은 국가의 발전에 도움이 되지 않을 것이다. 데이터 국지화는 가급적 지양하는 것이 타당하지만, 데이터 국지화를 불가피하게 입법하게 된다면 국가안보나 국민의 본질적인 기본적 자유와 권리를 현저히 해할 가능성이 있는 경우와 같이 제한적인 범위 내에서 추진하는 것이 바람직하다.

## Ⅴ. 국외 이전을 위한 법적 요건 강화 방안 검토

### 1. 개인정보 국외이전 규율의 기본방향

개인정보를 인류의 보편적 가치를 보호하기 위하여 법이 보호하고자 하는 대상으로 인식을 하게 되면, 해외로 우리 국민의 개인정보가 이전되어 처리되는 경우에도 기본적으로 개인정보를 보호하고자 하는 우리의 법을 해외 사업자나 개인정보 처리자에게도 적용하는 것이 타당할 것이다. 또한 개인정보에 대하여 보편적 법익의 보호라는 관점에서 접근하면, 외국 정부도 우리나라 국민의 개인정보를 보호하기 위한 노력을 해야 할 의무를 인정할 수 있다. 이처럼 인류 보편적 가치의 보호라는 측면에서 우리의 개인정보 보호법제를 국내외에 동등하게 적용하여 우리 국민을 포함한 전세계 시민의 개인정보 보호를 위한 법규범으로 작동시킬 필요가 있다. 아울러 미래 지능정보사회에서는 개인정보의 국가간 유통은 불가피한 흐름이고, 각국은 협력하여 자국민의 개인정보보호를 위한 노력을 하여야 한다. 지리적 한계를 넘어서서 전세계로 유통되는 개인정보를 효과적으로 보호함으로써 그 뒤에 연결 되어 있는 개인과 개인의 법익을 보호할 필요가 있다. 이를 위해서는 개인정보 국외이전에 대한 효과적인 규율체계를 구축할 필요가 있다. 이 때 합리적 범위 내에서의 개인정보의 국가간 이동을 최대한 보장할 필요성도 함께 고려하여야 할 것이다.

## 2. 개인정보의 국외이전에 관한 효과적인 규율체계 정립방안

현행 개인정보 보호법에 따르면, 우리 국민의 개인정보가 국외로 이전되는 것과 관련하여 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 일정 사항[110]을 정보주체에게 알리고 동의를 받아야 하며, 개인정보 보호법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하지 못하도록 금지하고 있다.[111] 국외로의 제3자 제공 행위 외의 개인정보 국외이전 행위에는 국내법 상의 개인정보의 처리에 관한 일반 기준이 적용된다. 결국 제3자 제공 형태의 국외이전 행위는 반드시 정보주체의 동의가 필요하다. 한편, 정보통신망을 통한 개인정보의 국외이전에 대한 규율은 개인정보 보호법과 상이하다. 즉, 기본적으로 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하지 못한다.[112] 정보통신서비스 제공자등은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함)·처리위탁·보관하려면 이용자의 동의를 받아야 한다.[113] 다만, 정보통신서비스의 제공에 관한 계약을 이행하고 이용자 편의 증진 등을 위하여 필요한 경우로서 일정한 고지사항[114] 모두를 개인정보처리방침을 통하여 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁·보관에 따른 동의절차를 거치지 아니할 수 있다.[115] 동의를 받아서 개인정보를 국외로 이전하는 경우에는 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.[116] 이처럼 정보통신망을 통하여 국외이전이 이루어지는 경우와 그 외의 경우에 국내법도 차별적인 취급을 하고 있기 때문에 이에 대한 일원화가 먼저

110) 동의를 받기 전에 고지해야 할 사항은 (1) 개인정보를 제공받는 자, (2) 개인정보를 제공받는 자의 개인정보 이용 목적, (3) 제공하는 개인정보의 항목, (4) 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간, (5) 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용이다. 개인정보 보호법 제17조 제2항 각 호.

111) 개인정보 보호법 제17조 제3항.

112) 정보통신망법 제63조 제1항.

113) 정보통신망법 제63조 제2항.

114) 고지사항은 (1) 이전되는 개인정보 항목, (2) 개인정보가 이전되는 국가, 이전일시 및 이전방법, (3) 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처), (4) 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간이다. 정보통신망법 제63조 제3항 각 호.

115) 정보통신망법 제63조 제2항 단서.

116) 정보통신망법 제63조 제4항.

이루어져야 할 것이다. 국내법 상 개인정보 국외이전에 대한 일원적 규율이 이루어지게 되면, 국외이전에 대한 규율의 기본 방향은 앞서 살펴본 것과 같이 국내 및 국외에서의 개인정보 처리에 관한 동등 규제로 설정되어야 한다. 그런데 개인정보의 국가간 이동 또는 해외 이전에 관하여 국내외 동등 규제 원칙을 기본 방향으로 설정한다고 하더라도 현실적으로 해외 사업자나 단체, 국가 등에게 우리의 개인정보보호 법제를 있는 그대로 모두 준수하라고 요구하는 것은 쉽지 않다. 나아가 우리의 개인정보보호 관련 법규정을 해외의 사업자에게 집행하는 것은 더더욱 쉽지 않다. 만일 해외 사업자가 스스로 국내 사업자와 마찬가지로 국내 개인정보보호 관련 법령을 준수하는 경우라면 동등 규제의 원칙에 따라 규율하면 될 것이다. 한편, 해외 사업자가 국내법제를 준수하지 않는 경우에도 법집행을 포기할 것이 아니라 가능한 우리 법체계로 편입시키고, 개인정보 침해나 국내법 위반이 발생되는 경우에 실질적인 구제가 이루어질 수 있도록 절차적인 보장을 꾀하는 방향으로 국외이전 규율체계를 정립할 필요가 있다. 이를 위해서는 먼저 EU[117]나 일본의 경우처럼 개인정보의 국가 간 이동을 합법적으로 허용하는 다양한 법적 근거를 마련하여 국내법 준수의 여지를 확대할 필요가 있다. 또한 해외 사업자가 스스로 구속력 있는 기업규칙을 제정하거나 적절한 안전조치 또는 공인된 인증 획득 등과 같이 개인정보보호를 위한 자발적 노력과 함께 피해가 발생한 경우에 구체적인 해결절차를 제공하는 경우에는 개인정보의 국외이전을 허용해주는 근거를 법적으로 제도화할 필요가 있다.

117) EU GDPR이 규정하는 국외이전에 관한 규율 내용은 최경진, “국제거래에서의 개인정보의 국가간 이동에 대한 소고 – EU, 미국, 일본의 최근 법제 동향을 중심으로 -”, 「국제거래법연구」 제26집 제2호(2017.12.), 83-88면 참조.

# 제2절 국제적인 공조체계 및 상호주의적 보호체계 구축

## Ⅰ. 국제적인 공조체계 확립

해외로 이전된 우리 국민의 개인정보를 보호하기 위한 1차적인 방안은 현 상태 그대로를 유지하더라도 행할 수 있는 국제적인 공조체계를 확립하는 것이다. 사실 주권국가의 영토를 넘어서 다른 나라에까지 법집행력을 행사하는 것은 쉬운 일이 아니다. 오히려 상대편 국가의 주권을 존중하면서, 우리 국민의 개인정보 보호가 이루어질 수 있도록 상대국가와 협력하고 상대국가가 직접 개인정보보호를 위한 노력이나 집행을 지원해주는 것이 더 바람직하고 현실적일 수 있다. 많은 나라가 주목하고 있는 EU GDPR도 국제협력의 중요성을 강조하여 다양한 국제협력 추진 사항을 규정하고 있다.[118] 즉, 제3국 및 국제기구와 관련하여 집행위원회와 감독기관은 다음과 같은 국제협력조치를 취하여야 한다.

| | |
|---|---|
| 1 | 개인정보 보호를 위한 법률을 효과적으로 집행하기 위한 국제협력 메커니즘(international cooperation mechanisms) 개발 |
| 2 | 개인정보와 기타 기본권 및 자유의 보호를 위한 적절한 안전조치(appropriate safeguards)를 조건으로, 통지, 민원 이첩, 조사 지원, 정보 교환 등을 통해 개인정보 보호를 위한 법률 집행에 대하여 국제 상호지원 제공 |
| 3 | 개인정보 보호를 위한 법률 집행 과정에서 국제협력을 촉진시킬 목적으로 행하는 논의 및 활동에 이해 당사자들을 참여시킬 것 |
| 4 | 제3국과의 사법 분쟁 등 개인정보 보호 법률 및 관행에 대한 교류 및 문서화를 촉진 |

우리나라도 개인정보 보호법 제14조와 정보통신망법 제62조에서 국제협력을 다음과 같이 규정하고 있다. 그러나 이들 규정은 추상적인 시책 마련의 선언적 규정처럼 운용되고 있다.

118) GDPR Article 50.

[개인정보 보호법]
**제14조(국제협력)** ① 정부는 국제적 환경에서의 개인정보 보호 수준을 향상시키기 위하여 필요한 시책을 마련하여야 한다.
② 정부는 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하여야 한다.

[정보통신망법]
**제62조(국제협력)** 정부는 다음 각 호의 사항을 추진할 때 다른 국가 또는 국제기구와 상호 협력하여야 한다.
1. 개인정보의 국가간 이전 및 개인정보의 보호에 관련된 업무
(이하 생략)

해외로 이전된 우리 국민의 개인정보보호와 관련한 문제는 현실적이고 사례중심적인 접근이 필요한 경우가 많다. 따라서 국제협력의 경우에도 고위급부터 실무 레벨에 이르기까지 매우 세밀하고 긴밀한 협력을 통한 실질적인 국민의 개인정보보호 노력이 요구된다. 따라서 현행 개인정보 보호법이나 정보통신망법과 같이 시책 수립 혹은 추상적 선언에 머무를 것이 아니라 보다 구체적인 책무나 의무를 부과하여 실질적으로 해외로 이전된 국민의 개인정보가 보호될 수 있는 법적 근거도 마련하고 실제로도 끈기 있게 집행해나가는 노력이 필요하다.

나아가 지능정보사회로의 발전적 전환을 견인하고 있는 ICT 강국으로서 우리나라는 국제사회에서 주도적인 공조체계 정립을 위한 노력을 할 필요가 있다. 특히 우리나라는 세계적으로도 찾아보기 드문 강력하고 촘촘한 개인정보보호법제를 갖추고 있다. 이러한 우리나라의 경험과 법체계를 바탕으로 하여 국제적인 공조체계의 정립을 위하여 보다 더 적극적인 노력을 기울인다면, 해외에서의 우리 국민의 개인정보 보호수준을 높이는데 도움이 될 것이다. 이러한 국제 공조체계 정립을 위한 주도적 노력은 단기간에 가시적인 성과를 내기는 어려울 수 있지만 중장기적 측면에서 우리 법제를 글로벌 기준으로 만들어 나감으로써 해외에서의 개인정보 보호 수준을 높이는데 기여할 뿐만 아니라 국제사회

에서의 리더십을 바탕으로 우리 국민의 개인정보보호수준을 높이는데 실질적으로 기여할 수 있게 된다.[119]

## Ⅱ. 국제협약 추진 방안

개인정보 보호법은 국내에서의 합법적 처리기준과 관련하여, 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있는 근거로서 "조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우"를 규정한다.[120] 개인정보의 수집 및 이용의 경우에는 헌법에 의하여 체결·공포된 조약과 일반적으로 승인된 국제법규는 국내법과 같은 효력을 가지기 때문에[121] 이를 근거로 개인정보의 수집, 이용, 제공이 가능하다. 이러한 국내법 상의 규정을 해외 사업자 등에게 직접 적용되도록 노력한다고 하더라도 국가간의 주권의 존중이나 국제법 질서 등을 고려할 때 현실적으로 그 실행이나 집행은 쉽지 않다. 따라서 우리 국민의 개인정보가 많이 이전되는 국가나 우리와 경제적인 교류가 활발한 국가들이 공동으로 개인정보의 국외이전 및 상대국 내에서의 개인정보의 보호 수준 제고를 위한 다자간 또는 양자간 국제협약이나 행정협정 등을 추진할 필요가 있다. 국제협약을 체결하게 되면, 그 구체적인 내용에 따라서 보호수준이 달라지겠지만, 국제협약이 없는 상태와 비교할 때 보다 명확하고 집행 가능한 법적 근거가 생겨나기 때문에 우리 국민의 개인정보가 국외로 이전됨에 따른 보호수준을 높이는데 크게 기여할 수 있을 것이다. 이러한 국제협약의 체결은 국제적인 공조체계의 구축 및

119) 국제적인 공조체계의 확립을 우리나라 주도로 해야할 필요성에 대하여 최경진, "개인정보 국외이전에 관한 소고", 「법학논총」 제20집 제1호(2013), 58면은 "기존 프라이버시 및 개인정보보호 관련 공조체계에서 한국의 역할을 강화하는 것도 필요하지만, ICT분야의 선도국가이자 글로벌 시장에서 중요한 위치를 차지하는 우리나라의 위상에 맞게 한국 주도로 미국-EU-중국-일본 등을 아우르는 협력체계를 구축하여야 한다. 특히 국제적인 개인정보보호는 국내법의 강화보다 국제적인 공조가 더욱 효과적이고 실효성 있기 때문에 이러한 국제적인 공조체계의 마련은 매우 중요하고 시급하다. 이런 관점에서 가칭 "World Personal Information Emergency Readiness Scheme (World PIERS)"의 정립 및 한국 주도를 적극 추진하여야 한다"고 한다.

120) 개인정보 보호법 제18조 제2항 제6호.

121) 대한민국헌법 제6조 제1항.

운용 과정에서 이루어질 수도 있고, 국제협약의 체결과 국제적인 공조체계의 구축이 동시에 논의되어 실행될 수도 있다. 어느 경우이든 우리 국민의 개인정보를 글로벌 수준에서 효과적으로 보호하기 위해서는 정부가 다각적인 노력을 기울여야 한다.

## Ⅲ. 상호주의적 보호체계의 정립

해외로 이전된 우리 국민의 개인정보를 보호하기 위하여 개인정보보호에 관한 국내법을 해외 사업자나 단체 등에 직접 적용하기 위한 법제를 마련하고, 집행력 강화를 위한 외국 규제 기관과의 협력체계 구축 등을 통하여 우리 국민의 개인정보 보호수준이 높아질 수 있지만, 현실적으로 개인정보가 이전된 상대국이 협력을 하지 않게 되면 우리 법을 직접 적용하거나 집행하거나 쉽지 않다. 또한 개인정보보호를 위하여 전세계 모든 나라와 국제협약을 체결하거나 모든 국가가 참여하는 개인정보 보호를 위한 다자간 국제협정을 체결하는 것도 현실적으로 가능성은 매우 낮아 보인다. 오히려 우리나라와 교역을 많이 하는 나라이거나 선진국인 경우에는 우리 국민의 개인정보 보호수준이 상대적으로 높을 수 있다. 반면, 자유민주주의와 인권 보호가 충실하지 않은 나라의 경우에는 상대적으로 우리 국민의 개인정보보호가 용이하지 않을 가능성이 높다. 특히 후자의 경우에는 우리 법을 직접 적용하거나 집행력을 확보한다는 것은 더더욱 어려운 일일 것이다. 따라서 우리 국민의 개인정보를 효과적으로 보호하기 위한 간접적인 방도로서 상호주의에 기반한 대응방안을 도입하는 것도 고려해 볼만하다.

전통적인 의미에서의 상호주의는 다자간이든 양자간이든 무역협정에서 참여국 사이에서 쌍무적으로 제공하는 양허(reciprocal concessions)가 참여국 사이에서 균형을 이루는 것을 말한다.[122][123] 개인정보보호는 인류의 보편적 가치와 연계되어 있는 만큼 참여 국가

122) 국제법 맥락에서 상호주의의 역사와 전통적 상호주의 및 공격적 상호주의(aggressive reciprocity)의 상세한 개념과 분류에 대하여는 최병선, “국제무역에 있어서의 상호주의에 관한 고찰”, 「통상법률」제14호(1997.4.), 42-74면 참조.

123) 상호주의는 국제법의 생성과 집행에 매우 중요한 역할을 해왔고 관습 국제법이 가지는 보편성의 배경에 상호주의 원칙이 있다고 한다. 김화진, “국제법 이론의 역사와 현황”, 「저스티스」 통권 161호(2017.7.), 309면 및 321면.

사이의 대등한 등가적인 보호 수준의 확보라는 관점에서 상호주의 원칙은 해외 이전된 우리 국민의 개인정보보호에 유용한 수단이 될 수 있다.[124)125)]

즉, 우리 국민의 개인정보를 충실히 보호하는 국가일수록 해당 국가의 국민의 개인정보를 우리나라에서도 동등한 수준으로 보호해 주는 것이다. 반면, 우리 국민의 개인정보를 보호하지 않거나 침해가 많은 국가인 경우에는 해당 국가 국민의 개인정보의 처리에 관하여 국내에서 제공하는 보호수준을 그에 맞추어 낮추는 방안이다. 이러한 방안이 직접적으로 우리 국민의 개인정보보호 수준을 높여주지는 못하더라도, 적어도 우리나라와 국제교류를 하거나 무역을 하는 국가인 경우에는 간접적으로라도 상대국으로 하여금 일정 수준의 개인정보보호 수준을 갖추도록 압박하는 효과적인 수단이 될 수도 있다. 최근 정보통신망법의 일부 개정[126)]으로 제한적이지만 온라인 상의 개인정보보호와 관련해서 상호주의를 도입하였다. 이에 의하면, 개인정보의 국외 이전을 제한하는 국가의 정보통신서비스 제공자등에 대하여는 해당 국가의 수준에 상응하는 제한을 할 수 있다.[127)] 다만,

124) 이진규, "국제법상 조약관계에서 상호주의에 관한 고찰 - 1963년 「영사관계에 관한 비엔나협약」에 대한 미국의 실행을 중심으로", 「동아법학」 제78호(2018.2.), 363-364면에 따르면, "상호주의는 둘 이상의 국가들과 각 국가에 속한 개인들 간 흔히 발생하는 상호작용 속에서 정의와 신의성실을 준수할 것을 실효적으로 보장하게 하며 국가 간 법(law of nations)의 기초가 된다"고 설명한다. 이 보고서에서 말하는 국내법에 따른 상호주의 원칙 규정과 앞의 논문에서의 국제법 상의 상호주의 원칙 사이에는 차이가 있지만, 그 개념과 원리는 동일하다고 할 수 있다. 국내법에 따른 상호주의 원칙 규정의 경우에도 결국 상대 국가와의 사이에서 간접적이지만 개인정보보호를 위한 규범을 준수하고 정의와 신의성실을 준수하도록 실질적으로 보장하는데 기여할 것이다.

125) 문돈, "국제법의 준수와 작동메커니즘", 「국제정치논총」 제55권 제3호(2015.9.), 347면에 의하면, "대부분의 국제법이 상호주의에 입각한 분권화된 강제에 의존하고 있다"고 한다.

126) 법률 제15751호(2018. 9. 18.)로 일부개정된 정보통신망법이 2019.3.19.부터 시행된다. 이번 개정은 기본 취지는 "대한민국 국민이 글로벌 사업자에게도 국내 사업자에 대해 행사하는 것과 마찬가지로 본인의 개인정보에 대해 수집 · 이용 · 제공 등의 동의 철회, 열람청구, 정정요구 등 자기결정권을 실질적으로 행사할 수 있도록 하고, 방송통신위원회가 글로벌 사업자의 개인정보 침해 여부를 판단하기 위해 자료를 요청할 경우 필요한 자료를 신속하게 제출할 수 있도록 하는 한편, 글로벌 사업자가 대한민국 국민의 개인정보를 해외로 이전한 후 제3국으로 재이전 하는 등 해외 시장에서 유통되고 있음에도 법적 근거가 마련되어 있지 않고, 특히 우리나라보다 개인정보 보호 수준이 낮은 나라로의 이전에 대해서는 국제규범상 동등하게 보호하는 등 우리 국민의 개인정보가 해외에서도 안전하게 유통될 수 있는 방안을 마련하려는 것임"으로 밝히고 있다. 특히, 제63조의2(상호주의)를 신설한 배경으로는 국가별로 개인정보 보호 수준이 다르므로 수준에 맞게 합리적이고 탄력적으로 대응할 수 있도록 상호주의 규정을 도입한다고 밝히고 있다. 이번 개정에서는 상호주의 규정 신설 외에 개인정보보호를 위한 국내 대리인 지정제도와 국외 이전된 개인정보의 제3국으로의 재이전에 대한 동의 요건 신설이 포함되어 있다.

127) 개정 정보통신망법 제63조의2.

조약 또는 그 밖의 국제협정의 이행에 필요한 경우에는 예외로 한다. 이번 개정은 국외이전을 제한하는 국가에 대하여 그에 상응하는 수준으로 해당국가로의 우리 국민의 개인정보의 국외이전을 제한하는 것을 주된 내용으로 한다. 개정법은 상호주의의 입장을 채용하기는 하였지만, 제한적으로 국외이전 허용 수준에 상응하는 상호주의만을 도입하였을 뿐 전체 개인정보보호수준을 평가하여 그에 상응하는 수준의 보호를 꾀하는 일반적 상호주의적 대응방안을 규정하고 있지는 않다. 보다 효과적인 대응을 위해서는 국외이전에 대한 제한 수준의 평가에 머무르지 않고 전체 개인정보보호 수준을 검토하여 상호주의적 대응을 허용하는 방향으로의 입법적 전환도 가능하다.

korea
legislation
research
institute

# 제5장

# 결 론

# 제5장 결 론

전세계가 네트워크로 연결되고 국가간의 이동성이 증가하면서 우리 국민의 개인정보가 해외로 이전되어 처리되는 경우가 늘고 있다. 그런데 해외로 이전된 개인정보의 경우에는 그 처리 기준이나 절차 등이 불명확하거나 우리 국민의 개인정보가 오남용 되는 경우도 많다. 이 때문에 우리 국민의 개인정보를 해외에서도 효과적으로 보호하기 위하여 어떠한 정책방안을 수립하여 추진하여야 하는지에 대한 연구를 목적으로 이 보고서가 작성되었다. 효과적인 대응방안을 도출하기 위하여 우선 이 보고서에서는 자국민의 개인정보보호를 위한 개인정보보호법제의 해외 사례를 살펴보았다. 특히 최근 전세계적인 주목을 받고 있는 EU GDPR과 일본의 개인정보보호법을 살펴보았다. 아울러 개인정보나 국가안보 등 중요한 국가의 이익을 보호하기 위한 방안으로서 데이터 국지화 법제에 대하여도 중국, 러시아, 캐나다 등을 중심으로 살펴보았다. 또한 외국인의 개인정보의 열람에 대한 해외 법제로서 EU GDPR이 규율하는 내용과 최근 미국에서 제정된 CLOUD Act의 내용도 살펴보았다. 이러한 해외 사례에 대한 검토를 바탕으로 우리 법제 하에서의 해외에서의 우리 국민의 개인정보처리에 관한 규율 사항을 분석해본 후, 해외에서의 우리 국민의 개인정보의 효과적인 보호를 위한 법제도 개선방안을 도출하고자 시도하였다. 그 결과 사전적 대응방안으로서 국외이전을 원칙적으로 금지하면서 국외이전 요건을 설정하는 방안, 데이터 국지화 규제 방안, 국제공조체계 확립 방안, 피해구제체계 마련 방안 등의 추진 가능성을 검토하였다. 아울러 국가간 대등한 등가적 개인정보보호수준의 확보라는 관점에서 상호주의 원칙에 기반한 개인정보보호 방안의 가능성에 대하여도 살펴보았다. 이상의 다양한 대응수단은 국민의 개인정보의 해외 이전에 대응한 상당한 보호수준을 확보하는데 도움이 될 수도 있지만, 자칫 무역을 근간으로 삼는 우리나라의 경우에

국가간 무역을 저해하는 요인으로 작용할 가능성도 배제할 수 없다. 따라서 국민의 개인정보의 국가간 이전도 적절히 허용하면서도 우리 국민의 권익이 침해되지 않고 적절히 구제받을 수 있도록 적절한 수준의 대응방안을 추진하여야 한다.

# 참고문헌

# 참 고 문 헌

강준모, “우리나라FTA와 전자금융법제”, 한국법제연구원, 2010. 10.

경성대학교 산학협력단, 일본의 개인정보보호 법제・정책 분석에 관한 연구, 개인정보보호위원회, 2017.12.

구태언, “개인정보 국외 이전제도의 현황 및 개선방안 연구”, 가천법학 제6권 제1호, 가천대학교 법학연구소, 2013.

김인석, “국제적 상호운용성 강화 및 지능정보화 시대에 부응한 개인정보보호 발전 방안 연구”, 개인정보보호위원회 정책연구용역 연구보고서, 개인정보보호위원회, 2016

김진환, “개인정보 보호의 규범적 의의와 한계”, 한국법학원, 저스티스 제144호, 2014.10.

김현경, “데이터 속성과 국지화 규범의 법적 쟁점에 대한 고찰”, 토지공법연구 제78집, 2017.5.

김화진, “국제법 이론의 역사와 현황”,「저스티스」통권 161호, 2017.7.

노현숙, “EU 개인정보 국외 이동 규정의 유용성”, 법학논총 제36집, 숭실대학교 법학연구소, 2016

문 돈, “국제법의 준수와 작동메커니즘”,「국제정치논총」제55권 제3호, 2015.9.

박영우, “글로벌 기업에 대한 개인정보보호 규제효과 제고 및 불법・청소년유해정보의 유통금지를 위한 국가간 협력방안 연구”, 방통융합정책연구 연구보고서, 방송통신위원회, 2014

박훤일, “개인정보의 현지화에 관한 연구”, 경희대학교 법학전문대학원, 경희법학52권 4호, 2017.12.

북경경도법률사무소(King&Capital Lawfirm), “중국 사이버보안법 관련 법규 해설”, 한국무역협회 북경지부, 2017.6.

송영진, “미국 CLOUD Act 통과와 역외 데이터 접근에 대한 시사점”, 형사정책연구 제29권 제2호(통권114호), 한국형사정책연구원, 2018.

오길영, “클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률안의 검토와 비판”, 민주주의법학연구회, 민주법학 56권0호, 2014.11.

윤경선, “글로벌 인터넷 검열ㆍ통제 동향과 시사점”, 한국정보화진흥원, 2017.10.

윤재석, “유럽연합과 미국의 개인정보 이전 협약(프라이버시 쉴드)과 국내 정책 방향”, 정보보호학회 논문지 제26권 제5호, 한국정보보호학회, 2016

이진규, “국제법상 조약관계에서 상호주의에 관한 고찰 - 1963년「영사관계에 관한 비엔나협약」에 대한 미국의 실행을 중심으로”,「동아법학」제78호, 2018.2.

이창범, “한국의 개인정보 국외이전 법제 현황과 개정방향”, 법학논총 제36권 제3호, 전남대학교 법학연구소, 2016

최경진, “개인정보 국외이전 법제 정비방안”, 연구보고서, 한국인터넷진흥원, 2012.

최경진, “개인정보 국외이전에 관한 소고”,「법학논총」, 제20집 제1호, 2013

최경진, “GDPR등 EU와 우리나라 온라인상 개인정보보호 법제 비교 연구”, 방송통신정책연구 연구보고서, 방송통신위원회, 2016.

최경진, “국제거래에서의 개인정보의 국가간 이동에 대한 소고 - EU, 미국, 일본의 최근 법제 동향을 중심으로 -”,「국제거래법연구」제26집 제2호, 2017.12.

최병선, “국제무역에 있어서의 상호주의에 관한 고찰”, 「통상법률」제14호, 1997.4.

최창수, “수사ㆍ정보기관의 통신이용 정보수집권에 관한 미국의 입법례와 그 함의 -「2015년 미국 자유법」에 대한 검토를 중심으로-, 한국정보법학회, 정보법학 제20권 제1호, 2016.05.

한국정보화진흥원(NIA) 보도자료, “새로운 데이터 경제 시대, 데이터 주권의 부상”, 2018.08.24.

한귀현. 일본 개정개인정보보호법의 주요내용과 그 시사점. 공법학연구, 18(4), 2017

한희원, “초국가적안보위협세력에의 법규범적 대응 법제연구 : 미국 애국법에 대한 고찰”, 중앙법학회, 중앙법학 12권2호, 2012.6.

행정안전부, “개인정보 보호법령 및 지침・고시 해설”, 2011. 12.

허진성, “데이터 국지화(Data Localization) 정책의 세계적 흐름과 그 법제적 함의”, 언론과 법 제13권 제2호, 2014.12.

EU Official Journal of the European Union issue L119, 2018.5.15.

Scott Livingston and Graham Greenleaf, “Data localisation in China and other APEC jurisdictions”, Privacy Laws & Business International Report Issue 143, October 2016.

日置巴美・横澤田悠・本間貴明, 前掲論文, 時の法令 第1996號, 2016. 2.

横澤田悠, 前掲論文, 法律のひろば 第69卷 第5號, 2016. 5.

## 참고 웹사이트

Amar Toor, Cutting the cord: Brazil's bold plan to combat the NSA,

http://www.theverge.com/2013/9/25/4769534/brazil-to-build-internet-cable-to-avoid-us-nsa-spying (2018.10.31. 최종방문)

Shaun Waterman, "Trans-Pacific Partnership will ban data localization laws", fedscoop in OCt 5, 2015. <https://www.fedscoop.com/tpp-will-ban-data-localization-laws/> (2018.10.31. 최종방문)

국가기록원, http://www.archives.go.kr (2018. 10. 31. 최종방문)

백지영, "美, 클라우드법 발효...사생활 침해vs공익 충돌 우려", 디지털데일리, 2018.03.27. 기사, <http://www.ddaily.co.kr/news/article.html?no=167178> (2018.10.31. 최종방문) 참조.

법제처, 국가법령정보센터, http://www.law.go.kr, (2018. 10. 31. 최종방문)

이종연 미국변호사, "미국 현행 통신 감청법 제도와 절차", 법률신문 오피니언 (2015.08.13.자), <https://www.lawtimes.co.kr/Legal-Opinion/Legal-Opinion-View?serial= 94910> (2018.10.31. 최종방문)

주로스앤젤레스 대한민국총영사관, "디지털 무역 이해하기 Ⅰ: 디지털 무역에서의 무역장벽" (2017.07) <http://overseas.mofa.go.kr/us-losangeles-ko/brd/m_4370/view.do?seq=1319204&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=> (2018.10.31. 최종방문)

허중혁, "일본 개인정보보호법 개정안 5월30일 전면시행", 법률신문 2017.3.22.자, <https://www.lawtimes.co.kr/Legal-News/Legal-News-View?serial=108889> (2018.10.31. 최종방문)

법제현안분석지원 현안대응 2-⑦

# 해외이전 우리 국민의 개인정보 보호 방안 마련 연구

2018년 11월 7일 인쇄
2018년 11월 9일 발행

발 행 인 | 이 익 현

발 행 처 | 한국법제연구원
세종특별자치시 국책연구원로 15
(반곡동, 한국법제연구원)
전 화 : (044)861-0300

등록번호 | 1981.8.11. 제2014-000009호

홈페이지 | http://www.klri.re.kr

값 7,000원



ISBN : 978-89-6684-897-3 93360

한국법제연구원
KOREA LEGISLATION RESEARCH INSTITUTE

세종특별자치시 국책연구원로 15 (반곡동, 한국법제연구원)
T.044)861-0300 F.044)868-9913 http://www.klri.re.kr



93360
ISBN 978-89-6684-897-3
값 7,000원