2024 Vol. 4

PRIVACY REPORT

2024 개인정보 이슈
심층 분석 보고서

개인정보 국외이전

KISA 한국인터넷진흥원

PRIVACY REPORT

2024 개인정보 이슈 심층 분석 보고서

| CONTENTS |

2024 Vol. 4

국외이전

데이터 안보 논의의 동향과 시사점

미국의 행정명령과 관련 조치를 중심으로

김상배
서울대학교 교수

1. 데이터 국외이전 이슈의 전환

최근 미중 디지털 패권경쟁이 가속화되고 있는 가운데, 첨단기술 경쟁 못지않게 큰 주목을 받는 미중 양국 간 이슈 중의 하나가 데이터의 국외이전을 둘러싼 논란이다. 특히 최근 데이터 국외이전 이슈의 초점이 '경제'에서 '안보'로 전환되고 있음에 주목할 필요가 있다. 이전에는 중국의 시각에서 미국 기업에 의한 데이터의 국외 유출을 경계하는 것이 관건이었다면, 최근에는 미국 정부가 나서서 중국 제품과 서비스를 통한 데이터 안보의 침해를 거론하는 국면으로 이행하고 있다. 다시 말해, '디지털 경제'의 관점에서 본 '데이터 주권'으로부터 '국가안보'의 관점에서 본 '데이터 안보'로 이슈의 전환이 발생하고 있는 것이다.

데이터 안보 논의가 내세우는 담론은 '신흥안보(emerging security)'의 시각에서 본 '안보화(securitization)'이다. 데이터 분야에서 '안보'를 논하지만, 이는 전통적인 군사안보의 내용을 담은 데이터만 문제 삼는 것은 아니다. 빅데이터 세상에서는 국가안보와 무관해 보이는 민간 데이터의 '안전'과 집단 차원의 '보안' 문제가 언제든지 지정학적 시각에서 본 국가적 '안보' 문제로 '창발(emergence)'할 수 있기 때문이다. 이에 근거하여 미국은 최근 중국산 '제품'의 수입규제에서 '서비스'의 사용금지로, 그리고 '데이터 자체'의 이전금지로 '안보화'의 전선을 확대·심화하고 있다.

미국 정부가 국가안보라는 시장 외적 잣대를 동원해서 중국 기업들의 기술추격과 미국 시장 진입을 견제한다는 비난도 없지 않다. 그러나 중국으로의 데이터 유출 그 자체가 미국에 큰 자원 손실이자 안보 위협이 되는 것도 엄연한 사실이다. 중국이 국가주권 논리를 내세우며 이미 인터넷상의 장벽을 세운 마당에, 미국마저 국가안보 논리에 기대어 데이터 유통을 통제한다면, '스프린터넷(Splinternet)'*의 세상이 현실화될 수도 있다. 이러한 와중에 한국은 미중 갈등의 사이에서 데이터 주권 이슈와 데이터 안보 이슈를 동시에 챙겨야 하는 처지에 놓이게 되었다.

* 'Splinternet'이라는 용어는 '쪼개진다(split)'와 '인터넷(Internet)'의 합성어다. 2018년 에릭 슈밋 전 구글 회장은 이러한 Splinternet의 등장 가능성을 언급한 바 있는데, 그는 인터넷 세계가 미국 주도의 인터넷과 중국 주도의 인터넷으로 쪼개질지도 모른다고 예견했다.

2. 미중 데이터 안보 갈등

미중 간에 데이터 안보와 관련해서 논란이 된 사건은 여럿 있지만, 그중에서도 2018~2019년 중국 화웨이의 5G 이동통신 장비를 둘러싸고 터진 갈등이 가장 대표적이다. 중국산 드론과 감시용 CCTV를 통한 데이터 유출이나 안면인식 AI를 활용한 데이터 감시·통제도 쟁점으로 불거졌다. 이외에도 네트워크에 연결된 거의 모든 중국산 제품에 '백도어'*가 있다는 의심이 끊임없이 제기되었다. 스마트폰부터 스마트TV, CCTV와 홈캠, 가정용 네트워크 공유기, 노트북, 심지어 키보드와 마우스 등 네트워크를 사용하는 대부분의 중국산 제품에 백도어가 숨어 있고, 이는 '펌웨어'** 업데이트를 통해서 활성화된다는 의심이었다. 향후 생성형 AI의 '딥페이크'도 초유의 데이터 안보 문제를 초래할 것이고, 인공위성의 정보·데이터도 새로운 안보 논란을 일으킬 것으로 예견된다.

* '백도어(Back door)'는 컴퓨터 시스템이나 소프트웨어에 정상적인 인증 과정을 우회하여 접근할 수 있는 통로를 의미하는데, 이는 개발자나 관리자의 유지 보수를 위해 만들기도 하지만, 해커들이 불법적으로 시스템에 침입하는 데 사용되기도 한다.
** '펌웨어(Firmware)'는 기기에 내장된 프로그램 소프트웨어를 의미하며, '펌웨어 업데이트'는 기기의 기능 개선, 버그 수정, 보안 강화 등을 위해 펌웨어를 최신 버전으로 갱신하는 과정을 지칭한다.

최근 미국 정부의 정책적 행보를 보면 데이터 이슈를 안보화하는 추세가 가속화되고 있음을 알 수 있다. 데이터 안보는 미중경쟁의 미래를 가늠하는 시금석이라고 할 수 있는데, 미국이 중국에 결코 양보할 수 없는 분야로 거론된다. 주된 논란거리는 국가안보 차원에서 중요한 미국의 핵심 데이터가 중국으로 유출될 수 있다는 우려이다. 2024년 들어 미국의 바이든 대통령이 데이터 안보와 관련해서 내린 행정명령과 관련 조치들이 눈길을 끈다. 한국에 주는 시사점이 큰 쟁점을 추려보면 ▲항만크레인 ▲민감한 개인정보 ▲동영상 플랫폼 ▲전자상거래 플랫폼 ▲'커넥티드카(Connected Car)' 등의 다섯 가지에 주목할 필요가 있다.

3. 중국산 항만 크레인 규제

2023년 3월 미 국방부와 정보당국은 미국 항구마다 설치돼 있는 중국의 항만 크레인에 대한 사이버 위협 가능성 조사를 시작했다. 미국이 특히 우려한 것은 중국 국영기업인 상하이진화중공업(ZPMC, Shanghai Zhenhua Heavy Industries Company Limited)의 항만 크레인이었다. ZPMC는 전 세계 크레인 시장의 약 70%를 차지하고 있다. 납품하는 국가 수도 100개국 이상이고, 미국에선 80%가 ZPMC 크레인을 사용 중이다. 이들 크레인에는 이동 물자의 출처와 행방을 등록 및 추적할 수 있는 센서가 달려있어서 중국 본사에서 크레인 현황을 모니터링할 수 있다는 의혹이 제기되었다. 이러한 스파이 논란 이후 1년 만에 미국 정부는 해양·항만의 데이터 및 사이버 안보를 강화하는 종합대책을 내놓았다.

결국 2024년 2월 21일 바이든 대통령은 데이터 안보와 사이버 위협을 이유로 중국산 항만

크레인을 규제하는 행정명령(Executive Order 14116 “Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States”)에 서명했다. 이 행정명령을 통해 해양 사이버 안보 위협에 대응하는 국토안보부의 권한이 확대되어, 해킹 사고 발생 시 보고를 요구하는 권한이 해안경비대에 부여되었다. 또한 미국 내 일부 항구에서는 ZPMC 크레인 소프트웨어가 다른 국적의 소프트웨어로 교체되었다. 아울러 바이든 행정부는 앞으로 5년간 크레인들을 미국산으로 대체하기 위해 200억 달러 이상을 투입하기로 했는데, 이는 미국이 30년 만에 자국 크레인 생산을 재개하는 결과를 낳게 되었다. 이러한 미국의 조치에 대해 중국은 미국이 힘을 남용해 중국 기업을 탄압하고 있다고 반발했다.

4. 민감한 개인정보 전송 금지

2024년 2월 26일 바이든 대통령은 유전자·위치 정보 등 미국인의 민감한 개인정보가 중국 등 우려 국가로 이전되는 것을 금지하는 행정명령(Executive Order 14117 “Preventing Access to Americans’ Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern”)에 서명했다. 이 행정명령은 미국의 데이터 기업들이 유전자 정보와 생체 정보, 컴퓨터 사용자의 키보드 입력 패턴, 개인 건강 데이터, 지리적 위치 데이터, 금융 데이터 및 특정 종류의 개인 식별 정보를 포함한 미국인의 민감한 개인정보를 중국, 러시아, 이란 등 ‘우려 국가’에 판매하는 것을 금지하는 내용을 담았다. 현재 미국에서는 데이터 브로커를 통해 데이터를 판매하는 것이 합법인데, 이러한 공백을 틈타 악의적인 행위자가 미국 시민의 데이터를 외국 정보기관에 전달하고 있다는 인식이 반영됐다.

민감한 개인정보의 보호는 이전부터 미중 양국 간의 주요 현안이었다. 2018년 미국 외국인투자심의위원회(CFIUS, Committee on Foreign Investment in the United States)는 알리바바 계열 중국 기업인 앤트 파이낸셜이 알리페이 결제 서비스와의 상승효과를 노리고 미국의 최대 송금 서비스 업체인 머니그램을 인수하려던 계획을 제지했다. 금융 서비스 분야에서 미국 시민을 식별하는 데 사용할 수 있는 데이터 안보에 대한 우려 때문이었다. 마찬가지로 2019년 5월 중국 게임회사 쿤룬은 2018년에 인수했던 미국의 소셜미디어 그라인더를 2020년 6월까지 매각하겠다고 발표했다. CFIUS는 800여만 명의 미국인이 사용하는 세계 최대의 성(性)소수자 커뮤니티인 그라인더의 데이터가 중국으로 넘어가면 안보 위협이 될 수 있다며 매각 명령을 내렸기 때문이었다.

5. ‘틱톡 금지법’ 통과

중국 바이트댄스의 동영상 플랫폼 틱톡도 개인정보와 데이터 안보 이슈를 일으킨 대표적인 사례다. 2024년 3월 13일 틱톡의 유통·배포 금지법안(H.R. 7521 “Protecting Americans from Foreign Adversary Controlled Applications Act”, 이하 ‘틱톡 금지법’)이 미 하원을

통과한 데 이어, 4월 24일에는 미 상원을 통과했으며, 이어서 바이든 대통령이 이 법안에 서명했다. 중국 공산당 관련 콘텐츠가 여과 없이 미국 청소년에 노출된다는 점, 자국 사용자의 개인정보가 중국 정부에 유출될 수 있다는 점 등이 문제로 지적되었다. 이에 따라 바이트댄스는 6개월 안에 틱톡 사업권을 매각해야 하며, 그렇지 않으면 미국 앱스토어에서 틱톡을 다운로드할 수 없게 되었다. 이는 사실상 틱톡의 미국 내 사용을 금지하는 행보로 이해되어 큰 논란을 일으켰다.

틱톡은 전 세계 이용자 19억 명을 돌파했고, 미국 내 이용자도 4억 인구의 1/3에 해당할 만큼 많은 이들이 이용하고 있다. 이처럼 경제적 파급효과가 크고, 관련 사업 종사자도 많은 틱톡을 금지한 조치는 상당한 반발을 초래했다. 가장 큰 쟁점은 이 조치가 미국 수정헌법 1조가 보장하는 '표현의 자유'를 위배한다는 것이었다. 사실 트럼프 행정부 때부터 틱톡은 여러 번 미국에서 퇴출당할 위기를 겪었지만, 그때마다 '표현의 자유'를 방패 삼아 위기를 모면했었다. 2024년 '틱톡 금지법'에도 바이트댄스는 법안에 대한 이의를 제기하면서 적극적으로 나서겠다는 뜻을 밝혔다.

6. 중국 전자상거래 플랫폼 규제

2023년부터 중국 전자상거래 플랫폼이 개인정보 관리와 사이버 안보 문제로 경계 대상이 되었다. 이른바 'C-커머스(China commerce)'로 불리는 알리, 테무, 쉬인(알·테·쉬) 등 중국 전자상거래 플랫폼이 글로벌 차원에서 약진하고 있다. 이들 C-커머스는 각국 시장에서 점유율을 늘려가고 있을 뿐만 아니라 미국 업체인 아마존이 기존에 구축한 글로벌 전자상거래 질서를 재편할 조짐마저 보여주고 있다. C-커머스의 글로벌 시장 진출이 소비자 후생을 증대할 기회를 제공하는 것은 사실이지만, 이들의 사업 행태가 시장 질서를 교란하고 소비자 피해를 유발하는 요인으로 비판을 받기도 한다.

특히 미국은 소비자들의 개인정보 보호와 사이버 안보 위협을 주요 문제로 거론하며 C-커머스에 대한 규제를 강화하고 있다. 개인정보 유출이 사이버 범죄는 물론이고 이는 중국의 정치·사회적 영향력을 확장하는 도구로 악용될 소지가 다분하다는 문제의식에서 비롯되었다. 최근 미국 워싱턴포스트(WP, Washington Post)는 호주전략정책연구소(ASPI, Australian Strategic Policy Institute)가 발표한 보고서를 인용해, 중국 정부와 공산당을 대변하는 미디어가 테무 등 중국 플랫폼을 통해 개인정보를 입수하여 선전 작업에 활용한다고 주장하여 파문이 일었다. 이들 미디어가 해외 소비자들의 취향, 의사결정 방식 등과 관련된 정보를 활용해 중국에 유리한 허위정보를 퍼뜨린다는 것이 주요 논점이었다.

7. 중국산 커넥티드카 규제

2024년 2월 29일 바이든 대통령은 중국의 '커넥티드카'가 미국에 안보 위협을 초래하는지

조사하라고 지시했다. 커넥티드카란 무선 네트워크로 주변과 정보를 주고받으며 내비게이션, 자율주행, 운전자 보조 시스템 기능 등을 제공하는 '스마트카'를 말한다. 네트워크에 연결돼 있어 해킹 위험이 있고, 자율주행 센서 장비가 데이터를 기록하기 때문에, 중국산을 쓰면 데이터 유출 우려가 있다는 문제가 꾸준히 제기돼 왔다. 표면적으로는 국가안보를 내세웠지만, 저가 중국산 자동차의 미국 시장 유입을 원천 차단하기 위해 마련한 선제적 조치라는 해석도 나온다. 이를 기반으로 미 상무부 산업안전국(BIS, Bureau of Industry and Security)이 커넥티드카의 '정보통신기술·서비스(ICTS, Information and Communications Technology Services)' 공급망 조사를 진행했으며, 그 후속 조치로 2024년 9월에 중국산 커넥티드카 관련 규제 초안을 발표할 것으로 알려졌다.

그 결과에 따라 미국이 국가안보를 위협할 수 있다는 이유로 미국 내 자동차에서 특정 부품의 사용을 제한할 수 있게 된다. 특히 자율주행차와 커넥티드카에 중국 소프트웨어 사용금지를 제안할 전망이다. 이와 함께 미국 정부는 중국에서 개발된 최신 무선통신 모듈을 장착한 차량 금지 규정도 계획 중이다. 2023년 12월에는 중국산 자율주행차 핵심 센서 장비인 '라이다(LiDAR, Light Detection and Ranging)'*가 데이터 유출 시비의 표적이 되기도 했다. 라이다는 발사된 레이저가 사물에 반사돼서 돌아오는 시간을 측정해 사물과의 거리를 재는 센서로 자율주행차에 꼭 필요한 기술이다. 현재 거론되는 조치는 차량 데이터를 수집하는 소프트웨어와 시스템에 초점을 맞춰져 있지만, 향후 커넥티드카와 자율주행차 관련 하드웨어로 확장할 가능성도 큰 것으로 알려졌다.

* '라이다(LiDAR)'는 레이저 빛을 이용해 거리를 측정하고 환경의 정밀한 3D 표현을 생성하는 원격 감지 기술을 의미한다.

8. 한국의 전략적 고민

미국이 중국에 대해 데이터 안보의 칼날을 들이대는 상황에서, 미중경쟁 사이에 낀 한국의 전략적 고민도 깊어질 수밖에 없다. 실제로 한국은 이미 미중 5G 갈등의 와중에 화웨이 장비 도입 문제로 몸살을 앓았다. 국내에 들여온 중국산 드론의 정보 유출이 우려되면서 그 사용을 배제했고, 중국 서버로 연결된 CCTV의 백도어 위험성도 심각하게 거론되었다. 최근에는 기상청에 납품된 중국산 기상관측장비에서 악성코드가 발견되기도 했다. 중국산 크레인도 국내 항만의 절반가량을 장악하고 있다. 한국에서 틱톡은 아직 큰 소란을 일으키진 않았지만, 알리와 테무, 쉬인 등 중국 전자상거래 플랫폼의 개인정보 관리 부실은 분란의 소지를 안고 있다. 미국 정부는 커넥티드카에 중국 기술이 사용되는 것을 규제하려는 과정에서 한국 등 주요 동맹국들과 공조하는 방안을 모색하고 있다.

여러 분야에 걸쳐서 중국을 견제하는 데이터 안보의 전선에 동참하라는 미국의 요구가 명시화되고 있다. 한국이 중국산 제품과 서비스에 많이 의존하는 것은 사실이지만, 최근 미국과의 동맹에 무게중심을 두는 추세로 미루어 볼 때, 데이터 안보를 내세운 미국의 행보를

무시할 수만은 없다. 경제적으로 값싸다고 해도, 보안에 문제가 있으면 아무 제품이나 서비스를 쓸 수는 없게 될 것이다. 결국 한국은 가성비 좋은 중국산 제품·서비스를 사용할 것이냐, 아니면 동맹국인 미국의 안보 우려 기조에 동조할 것이냐를 놓고 고민해야 할 상황이 닥칠지도 모른다. '화웨이 사태' 당시에 그랬던 것처럼, 기술·경제적 선택이 아닌 안보·외교적 결정을 내려야 할 상황이 언제 발생할지 모른다.

9. 데이터 안보 발상의 필요

최근 데이터 안보를 거론하며 국내 여론을 들썩이게 한 사건은, 한일간에 발생한 '라인야후 사태'였다. 2023년 11월 발생한 개인정보 유출 사고를 계기로 일본 정부가 네이버를 상대로 라인야후의 지분 매각을 요구하는 행정지도를 내려 논란이 벌어졌다. 표면적으로는 라인야후의 신속한 사이버 및 데이터 안보 강화 조치에 대한 요구이지만, 실제로는 네이버와 소프트뱅크가 반분하고 있는 라인야후 지분구조 재조정 문제로 해석되면서 우리 국민 여론이 비등했으며 급기야 우리 정부도 직접 나서기에 이르렀다. 그런데 라인야후 사태의 본질을 조금 더 곰곰이 살펴보면, 데이터 안보 문제로 증폭된 데이터 주권의 문제가 그 바탕에 깔려 있음을 알 수 있다.

이러한 종류의 데이터 안보 이슈는 계속 불거질 것으로 보인다. 이러한 상황에 직면하여 개인정보·데이터를 안보·외교의 시각에서 보는 인식의 제고가 필요하다. 오랜기간 한국의 개인정보 국외 이전 체계는 동의 중심이었는데, 정보주체의 선택권을 존중한다는 점에서는 의미 있으나 개인이 알기 어려운 위험성 파악이나 안전성 보장에 대한 한계가 있다는 의견이 제기되어 왔다. 이에 지난 2023년 9월부터는 정부가 다른 국가의 개인정보 보호수준을 평가하여 국외이전을 허용하는 동등성 인정 제도가 신설되고, 예측 불가능한 위험 상황 등을 고려하여 국외이전 중지명령의 근거도 마련됐다. 이러한 움직임에서 한 발 더 나아가 이제는 개인정보·데이터의 국외이전을 새로운 안보의 프레임으로 봐야 하는 세상이 되었다. 게다가 데이터 안보는 미중 두 강대국 사이에서 한국이 고민할 동맹외교의 사안으로 부상했다. 새롭게 전개되는 '데이터 지정학'의 지평 속에서 안보·외교의 숨은 코드를 읽어내는 국가적 혜안이 필요한 때다.

참고 문헌

김상배. 2022.『미중 디지털 패권경쟁: 기술-안보-권력의 복합지정학』한울.

김상배. 2023. "플랫폼 지정학 시대의 중견국 전략: 한국의 디지털 플랫폼 전략에 주는 함의,『국가전략』29(4), pp.33-64.

김상배. 2024. "차이나 커머스와 플랫폼 국가 자본주의: 중국 전자상거래 플랫폼의 역습을 어떻게 볼 것인가?"『아시아 브리프』4(17), 서울대학교 아시아연구소.

김상배. 2024. "이슈PICK 쌤과 함께: 라인·틱톡 사태로 보는 데이터 안보 전쟁" KBS 2024년 7월 7일 방송. (URL: https://www.youtube.com/watch?v=GIdVAmhBnqE)

Alami I, A.D. Dixon, and R. Gonzalez-Vicente, et al. 2022. "Geopolitics and the 'New' State Capitalism. Geopolitics. 27(3), pp.995-1023.

Gray, Joanne. E. 2021. "The Geopolitics of 'Platforms': The TikTok Challenge." Internet Policy Review. 10(2), pp.1-26.

Rolf, Steve and Seth Schindler. 2022. "The US-China Rivalry and the Emergence of State Platform Capitalism." Environment and Planning A: Economy and Space, 55(5), pp.1255-1280.

클라우드컴퓨팅서비스 이용과 국외이전

김경하
제이앤시큐리티 대표

1. 들어가면서

클라우드컴퓨팅서비스(Cloud Computing Service)는 '분산처리기술' 및 '가상화기술'을 기반으로 네트워크, 서버, 스토리지, 응용프로그램 및 서비스와 같은 컴퓨팅 자원을 직접 구매·소유·관리할 필요없이 네트워크가 연결된 곳이라면 언제, 어디서나 편리하게 접근하여 온디맨드(on-demand) 방식으로 이용할 수 있게 해준다. 특히, 빅데이터, 인공지능의 확산에 따라 대용량의 데이터를 효과적이고 효율적으로 활용하기 위한 기반 기술 및 서비스로서 클라우드컴퓨팅서비스의 활용이 확대되고 있다.

이러한 장점은 반대로 개인정보 처리의 관점에서는 개인정보의 저장 위치를 명확히 파악하기 어렵고 개인정보의 국경 간 이동이 불투명한 방식으로 실시간적으로 발생할 수 있으며, 개인정보 침해 발생 시 책임소재가 불분명하다는 점 등 다양한 이슈를 야기[1]한다. 이에 여기에서는 클라우드컴퓨팅서비스의 주요 개념과 클라우드 환경에서의 개인정보 처리 및 국외이전의 형태 분석을 통해 클라우드컴퓨팅서비스 이용에 따른 개인정보 국외이전의 주요 쟁점 사항을 살펴본다.

2. 클라우드컴퓨팅서비스의 개념 및 주요 특성

"클라우드컴퓨팅"이란 집적 · 공유된 정보통신기기, 정보통신설비, 소프트웨어 등 정보통신자원을 이용자의 요구나 수요 변화에 따라 정보통신망을 통하여 신축적으로 이용할 수 있도록 하는 정보처리체계[2]로서, ①주문형 셀프서비스(On-demand Self-service), ②광범위한 네트워크 접속(Broad Network Access), ③리소스 풀링(Resource Pooling), ④빠른 탄력성(Rapid Elasticity), ⑤측정되는 서비스(Measured Service) 등의 주요 특성[3]을 가진다.

클라우드컴퓨팅서비스란 클라우드컴퓨팅을 활용하여 상용(商用)으로 타인에게 정보통신자원을 제공하는 서비스[4]로서 일반적으로 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS(Software as a Service)로 구분[5]할 수 있다[6].

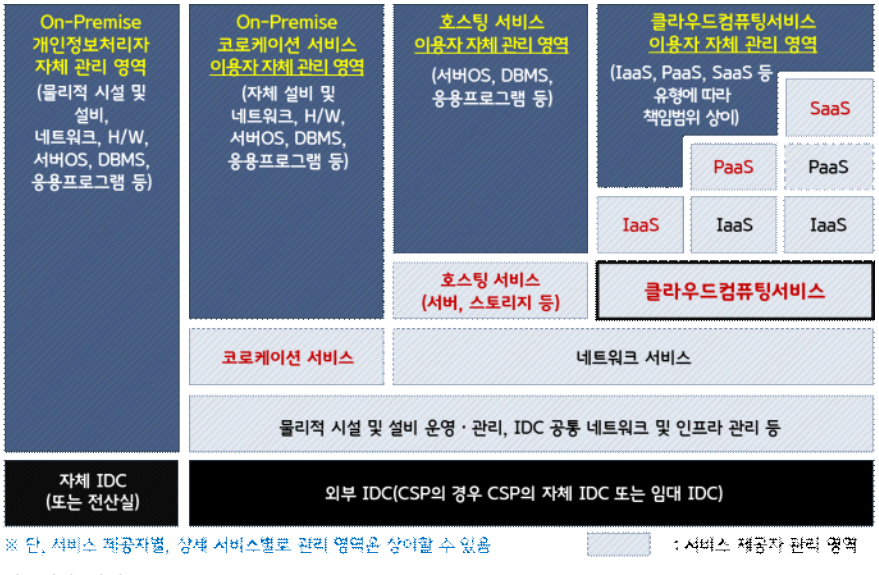
표 1 클라우드컴퓨팅서비스 주요 유형

구분	설명
IaaS	- 서버, 프로세서, 네트워크, 스토리지 등 인프라 스트럭쳐를 가상화 환경으로 만들어 필요에 따라 인프라 자원을 사용할 수 있도록 하는 서비스 클라우드컴퓨팅서비스 - 가상서버(Virtual Machine), 가상 스토리지, 가상 네트워크 등이 이에 해당함
PaaS	- 응용프로그램 등 소프트웨어의 개발 · 배포 · 운영 · 관리 등을 위한 환경을 제공하는 클라우드컴퓨팅서비스 - 관리형 DBMS, 관리형 WEB/WAS, 관리형 쿠버네티스 등이 이에 해당하며, IaaS 사업자가 관리형 서비스 형태로 함께 제공하는 것이 일반적임
SaaS	- 응용프로그램 등 소프트웨어를 제공하는 클라우드컴퓨팅서비스 - 고객관리 SaaS, 마케팅 SaaS 등이 이에 해당함 - 일반적으로 타 클라우드사업자의 IaaS 상에서 운영됨

3. 클라우드컴퓨팅서비스 환경에서의 개인정보 처리

개인정보처리자가 개인정보처리시스템을 구축·운영하는 방법으로는 아래의 그림과 같이 서버 등 장비를 직접 설치·운영하는 온프레미스(On-Premise) 방식과 호스팅 서비스(임대 방식), 클라우드컴퓨팅서비스 등 외부의 서비스를 이용하는 방식이 존재한다.

그림 1 개인정보처리시스템 구축·운영 방식 예시

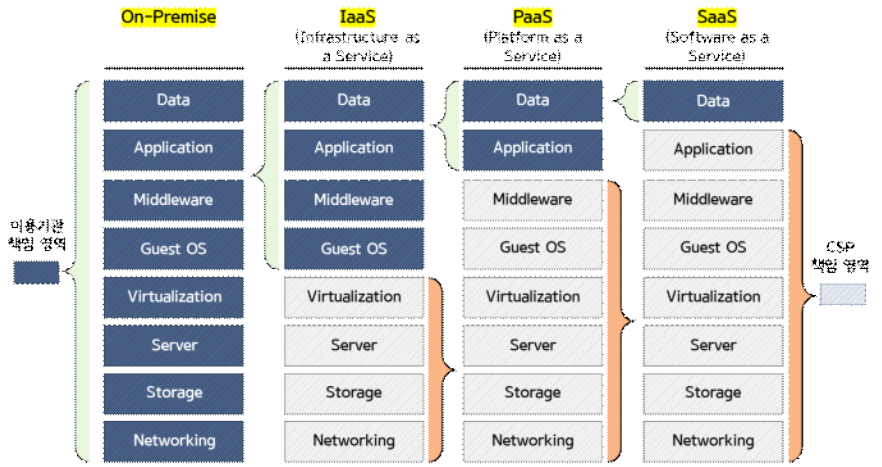


출처: 저자 작성

클라우드컴퓨팅서비스를 이용하는 방식을 선택한 경우, 개인정보처리자는 클라우드컴퓨팅서비스를 제공하는 자(이하 “CSP(Cloud Service Provider)”라 한다)의 IaaS, PaaS, SaaS 서비스를 단독 또는 복합적으로 이용하여 개인정보 처리업무 환경을 구성할 수 있다. 예를 들어, IaaS를 이용하여 대고객용 웹서버와 WAS서버를 구성하고, PaaS를 이용하여 관리형 DB에 개인정보를 저장·보관하고, SaaS를 이용하여 CRM 분석 및 정보주체 대상 대용량 메일발송 업무를 수행할 수 있다. 이 경우 클라우드컴퓨팅서비스 이용자는 개인정보처리자에 해당하며, 클라우드 환경에 구성된 웹서버, WAS서버, DBMS 등은 개인정보처리시스템에 해당되게 된다. 기존에는 자체 전산실 또는 데이터센터의 코로케이션서비스(상면서비스)를 이용하여 개인정보처리시스템을 독자적으로 구축·운영하는 온프레미스의 비중이 높았다고 한다면, 최근에는 클라우드컴퓨팅서비스를 이용하여 개인정보처리시스템을 구축·운영하는 방식의 비중이 크게 증가하고 있다.

온프레미스 환경에서는 개인정보처리자가 개인정보처리시스템의 구축·운영에 있어 물리적 영역에서부터 하드웨어, 운영체제, 미들웨어, 응용프로그램 등 전 영역에서 책임을 가지는 것에 비해, 클라우드컴퓨팅서비스를 이용할 경우 다음의 그림과 같이 IaaS, PaaS, SaaS 유형에 따라 이용자(개인정보처리자)와 CSP가 책임을 나누어 가지는 책임공유모델 또는 공동책임모델[7]이 적용된다.

그림 2 클라우드컴퓨팅서비스 유형별 책임영역



출처: 저자 작성

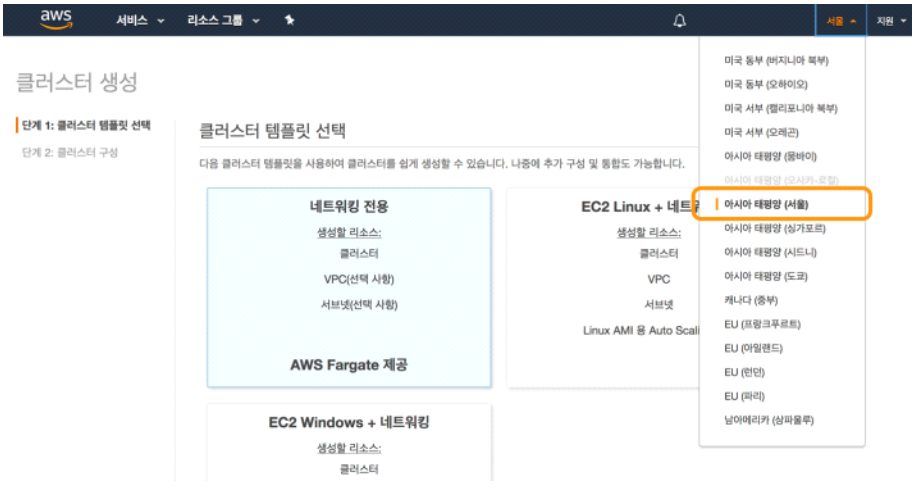
결국 이러한 책임공유모델에 따라 개인정보처리자와 CSP는 개인정보의 처리 및 보호에 있어 함께 관여한다고 할 수 있다. 다만 관여의 범위에 있어서는 IaaS, PaaS, SaaS에 따라 차이가 있을 수 있는데 IaaS의 경우 CSP가 가상화 레이어 하위의 영역을 관리함에 따라 개인정보의 보관 영역에 관여하게 되며, SaaS의 경우 사실상 개인정보처리시스템의 구성 및 운영 전반에 CSP가 관여한다고 할 수 있다.

4. 클라우드컴퓨팅서비스 환경에서의 개인정보 국외이전

클라우드컴퓨팅서비스는 분산처리 및 가상화 기술을 기반으로 하고 있다. CSP는 수많은 이용자에게 대규모의 서비스를 제공하기 위해 대용량의 저장능력과 고성능 컴퓨팅 능력을 효율적으로 제공할 수 있도록 여러 국가에 걸쳐 데이터센터를 세우고 가상화 환경 위에서 데이터를 분산 저장 및 처리하는 특성[8]이 있다.

개인정보처리자는 CSP가 제공하는 웹 기반의 클라우드 관리콘솔에서 데이터가 저장·처리되는 지역(Region)을 선택하는 것을 통해 간단하게 개인정보의 국외이전 여부를 설정할 수 있다. 기존에는 클라우드컴퓨팅서비스의 특성상 클라우드컴퓨팅서비스 이용자조차 데이터가 저장되는 위치 및 국가를 알기 어렵다는 우려가 존재하였지만, 현재는 IaaS와 PaaS의 경우에 일반적으로 클라우드컴퓨팅서비스 이용자인 개인정보처리자가 개인정보의 국외이전 여부를 직접 설정하고 관리할 수 있어 이러한 우려는 많이 해소된 상황이다. 물론 정보주체 입장에서는 클라우드컴퓨팅서비스를 이용하는 개인정보처리자가 개인정보 국외이전에 관한 사항을 정확하고 투명하게 공개하지 않는다면 자신의 개인정보가 이전되는 국가 등을 알기 어렵다는 문제점은 여전히 존재한다.

그림 3 클라우드 관리콘솔에서 지역(Region)을 선택하는 화면 예시[9]



출처: AWS(2018)

다음으로 개인정보처리자가 해외 SaaS를 이용하여 개인정보를 처리하는 경우 개인정보의 국외이전이 발생할 수 있다. 예를 들어, 개인정보처리자가 정보주체에게 SMS 문자 발송을 위해 해외 SaaS를 이용할 경우, 개인정보처리자는 국내에 위치한 개인정보처리시스템으로부터 문자 발송 대상자의 휴대폰번호를 추출하고 이를 API 등을 통해 해외에 위치한 SaaS 시스템으로 전송하고, SaaS에서는 해당 휴대폰번호를 대상으로 문자를 발송하게 된다. 이 과정에서 국내 정보주체의 개인정보(휴대폰번호)가 SaaS가 위치한 국가로 이전되게 된다. 이 경우

개인정보처리자는 SaaS 사업자가 위치한 국가를 사전에 파악할 수 있으나, SaaS 사업자가 이전받은 개인정보를 백업 등의 목적으로 다시 다른 국가에 재이전하고 있는지 여부는 확인이 어렵다는 문제점은 존재한다.

5. 클라우드컴퓨팅서비스 개인정보 국외이전과 관련된 주요 쟁점 사항

가. 개인정보 처리 및 국외이전에 있어 CSP의 법적 지위 문제

클라우드컴퓨팅 환경에서 개인정보를 처리할 경우 CSP의 법적 지위에 있어 모호한 측면이 존재한다[10][11]. SaaS의 경우 앞서 [그림 2]에서 살펴본 바와 같이 개인정보 처리의 대부분을 CSP가 담당하고 있어 개인정보처리자와 SaaS를 제공하는 CSP 사이에는 개인정보 처리업무 위수탁 관계가 형성된다는 것에는 큰 이견이 없는 것으로 보인다. 다만 IaaS의 경우 CSP는 단순히 컴퓨팅 자원만 제공하고 이용자의 데이터에는 접근하지 않으며, 이용자가 자신들이 제공한 자원을 이용하여 개인정보를 처리하는지 여부는 알 수 없기 때문에 개인정보 처리업무 위탁에 해당하지 않는다는 입장이 존재한다. 반면에, CSP가 이용자 데이터에 접근하지 않는 것은 기술적인 관점에서 원천적으로 불가능한 것은 아니며 결국 내부통제 등을 통해 관리하는 것이고, 최소한 개인정보의 저장 및 파기 등 일부 처리[12]에 대해 관여하는 것으로 볼 수 있어 개인정보 처리업무 위탁으로 볼 수 있다는 입장 또한 존재한다. 특히 개인정보처리자와 CSP가 직접 계약하지 않고 MSP(Managed Service Provider)를 통해 계약이 이루어질 경우 개인정보 위수탁 관계는 더욱 복잡해진다.

만약 CSP가 개인정보 처리업무 수탁자에 해당될 경우에는 개인정보 보호법 제26조에 따라 위수탁 계약, 개인정보 처리방침 공개, 수탁자 관리·감독, 재위탁시 위탁자 승인, 수탁자에 대한 준용 등의 요건이 적용되지만, 그렇지 않을 경우에는 이러한 요건의 적용이 배제된다.

다만, 개인정보 보호법 제28조의8에서는 국외이전의 유형을 국외 제공 및 처리위탁 뿐만 아니라 “보관”을 포함하고 있으며 해외 IaaS를 이용하는 경우 최소한 “보관”은 이루어지므로, 이 경우 해외 CSP는 개인정보의 국외이전을 받는 자에 해당한다고 볼 수 있다. 따라서 개인정보처리자는 개인정보 보호법 시행령 제29조의10제2항에 따라 개인정보 보호를 위한 안전성 확보조치, 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 조치 등의 사항에 대해 CSP와 미리 협의하고 이를 계약 내용 등에 반영하여야 할 것이다.

참고로 EU GDPR에서는 이용자가 클라우드컴퓨팅서비스를 이용하여 개인정보를 처리하는 경우 이용자가 컨트롤러로서 프로세서인 CSP와 데이터 처리 부칙(DPA, Data Processing Addendum)이 포함된 계약을 체결[13]하고, 클라우드컴퓨팅서비스를 이용하는 과정에서 국외이전에 발생할 경우에는 컨트롤러인 이용자와 프로세서인 CSP 사이에 표준계약(SCC,

Standard Contractual Clauses)을 체결함으로써 개인정보 국외이전에 따른 위험을 관리하고 있다는 점[14]은 우리 법제에서도 참고할 필요가 있다.

나. 클라우드컴퓨팅서비스 이용에 따른 국외이전 적법 요건 적용의 경직성 문제

개인정보 보호법 제28조의8 제1항에 따르면 개인정보처리자는 개인정보의 국외이전이 원칙적으로 금지되지만 ①정보주체의 별도 동의, ②법률·조약·국제협정에 국외이전에 관한 특별한 규정, ③정보주체와의 계약의 체결·이행을 위해 필요한 처리위탁·보관으로서 개인정보 처리방침을 통해 알린 경우, ④지정된 개인정보 보호 인증, ⑤국가차원의 인정 등 5가지 요건 중 하나에 해당될 경우 국외이전이 허용된다.

클라우드컴퓨팅서비스 이용과 관련하여 개인정보 국외이전시 정보주체로부터 별도 동의를 받는 것이 쉽지 않기 때문에 대부분 ③번을 적법 요건으로 활용하는 것이 일반적이다. 하지만 이 경우 정보주체와의 계약의 체결 및 이행을 위하여 개인정보의 처리위탁 · 보관이 필요한 경우가 전제되어야 하는데, 이렇게 판단하기 애매한 상황들이 다수 존재한다. 예를 들어, 데이터 백업이나 재해복구시스템 구성을 위한 경우에는 정보주체에게 제공하는 서비스의 가용성과 안정성을 보장하는 것으로서 계약의 이행을 위해 필요한 경우로 볼 수 있을 것이지만, CRM이나 DW(데이터웨어하우스) 구성, 인공지능 학습 등의 경우에는 정보주체와의 계약의 체결 및 이행을 위해 필요한 경우로 볼 수 있을지에 대해 논란이 있을 수 있다.

만약 "정보주체와의 계약의 체결 및 이행"을 좁게 해석할 경우, 사실상 정보주체의 별도의 동의를 받거나 그 외 다른 적법 요건을 적용하는 것이 현실적으로 어렵다는 점을 고려할 때, 클라우드컴퓨팅서비스를 통한 개인정보 국외이전에 상당한 제약사항이 생긴다고 할 수 있다.

이러한 문제점은 현행 개인정보 보호법의 개인정보 국외이전의 적법 요건의 경직성에서 기인하는 것으로서, 표준계약조항(SCC) 등 적절한 안전장치를 전제로 정보주체 동의없이 개인정보의 국외이전이 가능한 요건을 좀 더 다양화할 필요가 있다.

다. CSP에 대한 개인정보 보호조치 적용 문제

만약 개인정보처리자가 해외 클라우드컴퓨팅서비스 환경에 개인정보처리시스템을 구성한 경우, 해당 개인정보처리시스템은 개인정보 보호법 제29조 및 시행령 제30조, 개인정보의 안전성 확보호치 기준에 따른 보호조치를 적용하여야 한다.

IaaS의 경우 CSP가 개인정보에 접근하지 않는다는 것을 전제한다면[15] 국내 개인정보처리자가 개인정보의 안전성 확보조치 기준에 맞게 클라우드 환경에서 개인정보처리시스템을 구축·운영하면 될 것이다. 그러나, SaaS의 경우 CSP가 개인정보처리시스템의 구축·운영의

대부분을 담당하고 IaaS와 달리 개인정보 처리업무의 위탁 여부가 명확함에 따라 개인정보의 안전성 확보조치 기준을 그대로 적용받게 된다고 할 수 있다.

그러나, 해외 SaaS의 경우 글로벌 서비스를 지향하기 때문에 인터넷망 차단조치, 접속기록의 보관 및 점검 등 국내에만 존재하는 개인정보의 안전성 확보조치 기준 요건을 모두 준수하는 것이 쉽지 않은 상황이며, 그렇다고 하여 해외 SaaS에 대해 예외를 인정할 경우 국내 사업자에 대한 역차별 이슈가 발생할 수 있어 바람직한 대안은 되지 못한다.

결국 점차 글로벌화 되어 가는 개인정보 처리환경을 반영하여 개인정보의 안전성 확보조치 기준을 이행하거나 또는 실질적인 위험에 근거하여 이에 상응하는 안전조치를 개인정보처리자가 선택하여 적용할 수 있도록 개인정보의 안전성 확보조치 기준의 유연성을 높이는 방안을 고려할 필요가 있다.

6. 맺음말

클라우드컴퓨팅서비스를 통한 개인정보의 국경간 이동은 앞으로도 더욱 확대될 것으로 보인다. 개인정보 보호법 2차 개정에 따라 개인정보의 국외이전 요건이 다양화되었지만, 클라우드컴퓨팅서비스의 맥락에서는 여전히 IaaS, PaaS, SaaS 등 유형별로 다양한 쟁점사항이 존재하며 점점 복잡해지는 양상을 보이고 있다. 이에 법제도적인 측면에서 클라우드컴퓨팅서비스 유형별로 CSP의 법적 지위를 명확화하고 표준계약조항 등 개인정보 국외이전이 가능한 요건을 추가하는 등 클라우드컴퓨팅서비스 환경에서 합리적인 기준과 절차에 따라 개인정보가 안전하게 이전될 수 있도록 할 필요가 있다. 또한, 개인정보처리자 입장에서도 개인정보 국외이전에 따른 리스크가 증가하는 추세에 있으므로, 현행 법체계에 대한 명확한 이해를 바탕으로 조직 내 개인정보 국외이전 현황을 정확히 파악하고 적법하고 안전한 국외이전이 이루어질 수 있도록 특별히 주의를 기울일 필요가 있겠다.

주석

[1] 정원준 “클라우드 컴퓨팅 환경에서 제기되는 개인정보 문제의 법적 고찰”, 法學論叢 第40卷 第1號, 2016.3.

[2] 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제1호

[3] NIST, “The NIST Definition of Cloud Computing (SP800-145)”, 2011.9

[4] 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호

[5] 이보성, 김범수, “클라우드 서비스 유형별 개인정보보호 방안”, Journal of The Korea Institute of Information Security & Cryptology, VOL.25, NO.5, 2015.10.

[6] 이 외에도 DaaS(Desktop as a Service), FaaS(Function as a Service), CaaS(Container as a Service), SECaaS(Security as a Service), AIaaS(AI as a Service) 등 다양한 형태의 클라우드컴퓨팅서비스가 출현하는 추세에 있다.

[7] 대다수의 CSP가 책임공유모델을 채택하고 있으며, 이용약관 및 SLA에 관련 내용을 포함하고 있다.

- AWS : https://aws.amazon.com/ko/compliance/shared-responsibility-model/ 참고
- MS Azure : https://learn.microsoft.com/ko-kr/azure/security/fundamentals/shared-responsibility 참고
- GCP : https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate?hl=ko 참고

[8] 예를 들어, 아마존웹서비스(AWS)의 경우 2024년 9월 기준으로 대한민국 서울리전을 포함하여 미국, 일본, 유럽, 중동, 아프리카 등 전세계에 34개의 리전을 운영하고 있다. (URL: https://aws.amazon.com/ko/about-aws/global-infrastructure/?p=ngi&loc=0 참고)

[9] AWS, “AWS Fargate, 서울 리전 출시”, 2018.11.9. (URL: https://aws.amazon.com/ko/blogs/korea/aws-fargate-now-available-in-seoul-region/)

[10] 강철하, “클라우드 환경에서 개인정보 국외이전의 법적 쟁점과 개선방향”, 경제규제와 법(Journal of Law & Economic Regulation) 제10권 제2호 (통권 제20호). (Vol. 10.

No. 2). 2017. 11. pp.301~327

[11] 김형섭, “클라우드컴퓨팅에서의 개인정보 보호에 관한 법정책적 검토”, (社)韓國法政策學會法과 政策硏究 第21輯第4號, 2021.12.

[12] 개인정보 보호법 제2조제2호 : “처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

[13] AWS, “AWS 데이터 처리 부칙(DPA)”, 2020.12. (URL: https://docs.aws.amazon.com/ko_kr/whitepapers/latest/navigating-gdpr-compliance/aws-data-processing-addendum-dpa.html)

[14] 박노형, 개정된 개인정보보호법상 개인정보의 국외이전에 관한 규정의 분석: GDPR을 참조하여“, 고려법학 제109호 2023.6.

[15] 그럼에도 불구하고, IaaS 환경에서 CSP가 개인정보 등 이용자 데이터에 접근할 가능성을 완전히 배제하기는 어려울 수 있다.

개인정보 국외이전을 위한 제도 설계

– 신뢰 기반의 국외이전

윤주호
법무법인(유한) 태평양 변호사

1. 개인정보 국외이전 관련 제재들

올해 8월 네덜란드 개인정보 감독기관(AP, Autoriteit Persoonsgegevens)은 차량공유업체 Uber Technologies Inc.와 Uber B.V. (이하 총칭하여 '우버')에게 운전자의 민감정보를 미국으로 이전하면서 유럽의 국외이전에 관한 조항들을 준수하지 아니하였다는 이유로 2억 9천만 유로(약 4,300억 원)의 과징금을 부과하였다.[1] 현재 우버는 네덜란드 위 결정에 대해 항소를 한 상태로 알려져 있다. 또한, 한국에서도 최근 전자금융업자가 해외 기업들에게 법에 따른 절차를 지키지 아니하고 개인정보를 이전하였다고 하여 조사가 진행되고 있다.

2. 개인정보의 국외이전을 위한 고려요소

글로벌 경제의 발전과 개인정보를 포함한 다양한 데이터를 이용하는 서비스의 증가로 인해, 개인정보의 국외이전에 관한 필요가 증가하고 있다. 그러나 정보주체의 입장에서 보면, 자신의 정보가 다른 국가로 이전되는 경우 그 국가에서 개인정보가 잘 보호되고 있는지에 대한 우려를 하게 된다. 한편, 규제당국의 입장에서도 해외로 이전되는 정보가 자국의 법률에 따라 적절히 보호되고 있는지, 혹은 법규 위반 사항이 발생하는 경우 그에 대한 시정을 요구할 수 있는지에 대한 고려를 하게 된다. 따라서 개인정보의 국외이전 제도는 이렇게 정보주체, 기업, 규제당국의 이해를 조화롭게 반영하여 설계되어야 한다.

한편, 개인정보의 국외이전 제도와 관련하여 "개인정보 및 정보보호 프레임워크의 상호운용성(Interoperability)[2] 확대"라는 용어와 "신뢰 기반의 자유로운 데이터 이동(Data Free Flow with Trust, 이하 DFFT)"라는 용어를 많이 접하게 된다. 먼저, 상호운용성 확대는 공식적으로 2013년 OECD의 "OECD Recommendation concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data(이하 "OECD Privacy Guidelines")"에서 등장하였는데, 구체적으로는 2013년 개정된 OECD Privacy Guidelines 제21조에서 상호운용성에 관하여 "회원국들은 본 가이드라인에 실질적인 효과를 부여하는 프라이버시 프레임워크 간의 상호운용성을 촉진하는 국제적 협약의 개발을 장려하고 지원하여야 한다(저자 번역)[3]"라고 추가 하였다.

당시 OECD는 이러한 상호운용성에 대해 명확히 정의하지 아니하였으나, 2021년 "Report on the Implementation of the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data"에서 "interoperability"에 관하여 "일관된 정보보호를 보장하며 국외이전을 촉진시키기 위한 개인정보 법제 또는 프레임워크의 기능"이라고 설명한 바 있다.[4]

다른 한편, 최근에는 G20, OECD에서 "신뢰 기반의 자유로운 데이터 이동"이라는 의미의 DFFT(Data Free Flow with Trust)라는 용어를 많이 사용하고 있는데, 이러한 DFFT는 2019년 일본에서 개최된 G20에서 당시 아베 총리가 글로벌 아젠다로 제기한 이후, G20 등에서 논의가 시작되었다. 당시 일본에서 언급한 DFFT는 글로벌 경제의 변화에 따른 국경 간 이전에 따른 개인정보 보호 및 지식재산권에 대한 내용까지를 포함하고 있었다. 하지만 해당 시점에는 DFFT를 위한 프레임워크 등이 구체적으로 논의되지는 않았다. 이후 2023년 G7 장관 회의에서 DFFT를 위해 실용적이고 유동적이며 상호운용 가능한 프레임워크의 구현 필요성이 제기되었으며, 이를 여러 법적 프레임워크, 가이드라인, 표준, 기술 등을 통해 달성할 수 있다는 점이 논의되었다.[5][6]

결국 DFFT는 개인정보 보호 제도의 상호운용성 확대를 포함하는 개념으로, 개인정보를 안전하게 보호하면서 국외이전을 원활하게 할 수 있는 국가 내 시스템 구축을 위한 노력, 또는 이를 위한 컨셉으로 이해될 수 있는데, 이러한 시스템 구축은 결국 앞에서 설명한 세 당사자의 이해를 고려하여 설정되어야 할 것이다.

3. 개인정보 국외이전을 위해 현재까지 마련된 제도들

가. 국제 및 지역 협정

개인정보 국외이전을 위해 상호운용성을 확대하는 방안 또는 정보주체 및 국가 간 규제기관의 신뢰를 확보하기 위한 방안으로 우선 국제 및 지역 간 협정을 고려할 수 있다. 지역 간 협정으로는 APEC 프라이버시 프레임워크(APEC Privacy Framework)[7]와 ASEAN 데이터관리프레임워크(ASEAN Framework on Digital Data Governance)[8]를 고려할 수 있다. 다만, 이러한 지역 간 협정은 회원국 국가들의 법제화를 통해서만 법률적 효력을 가지게 되는 일종의 권고로서, 지역 간 협정만으로 개인정보의 국외이전이 촉진되거나 개인정보의 보호 정도가 높아지지는 않고, 그 실천을 위한 개별 국가의 노력이 필요하다.

나. 이전되는 국가의 정보보호 수준에 대한 인정

GDPR 제45조에서는 제3국 또는 국제기구가 적정한 개인정보 보호 수준을 가지고 있는 경우에

는 EU 집행위원회(EU Commission)의 결정에 따라, 그 국가 또는 국제기구로의 정보 이전을 허용하고 있다.[9] 즉, EU 수준으로 개인정보를 보호하고 있다는 EU의 적정성 결정을 받은 국가로의 개인정보 이전은 정보주체의 권리를 침해할 가능성이 낮다는 점에서 다른 법적 근거가 없더라도 허용하고 있는 제도이다.

이러한 국외이전 제도는 한국에서도 동등성 인정 제도의 형태로 도입되었다. 즉, 개인정보 보호법 제28조의8 제1항 제5호는 "개인정보가 이전되는 국가 또는 국제기구의 개인정보 보호체계, 정보주체 권리보장 범위, 피해구제 절차 등이 이 법에 따른 개인정보 보호 수준과 실질적으로 동등한 수준을 갖추었다고 보호위원회가 인정하는 경우" 개인정보를 국외로 이전할 수 있다고 규정하여, 이전되는 국가의 정보보호 수준에 대한 인정을 통해 개인정보의 국외이전을 허용하고 있다.

다. 이전받는 기업의 정보보호 수준에 대한 인증

1) 구속력 있는 기업 규칙(Binding Corporate Rules, BCR)

GDPR 제46조 제2항 (a)호는 구속력 있는 기업 규칙을 개인정보 국외이전의 적법한 근거로 채택하고 있다. 그리고 구속력이 있는 기업 규칙으로 인정되기 위해서는 법적으로 구속력이 있어야 하며, 해당 기업집단의 모든 기업에게 적용이 강제되어야 한다. 또한, 이러한 구속력이 있는 기업 규칙이 있다는 점만으로는 부족하고 관련 규제 당국이 이러한 기업 규칙을 통해 정보주체의 권리 및 개인정보를 충분히 보호할 수 있다는 점에 대한 인증이 이루어져야 한다(GDPR 제47조).

2) Cross Border Privacy Rules(CBPR) 인증

현재 한국이 채택하고 있는 APEC CBPR 인증제도는 APEC 프라이버시 보호 원칙을 기반으로 기업의 개인정보 보호 체계를 평가하여 그 적합성을 인증하는 제도로서,[10] APEC 회원국 간 개인정보의 국외이전을 허용하는 매커니즘이다.

이러한 CBPR 제도는 국가가 아닌 개별 기업에 대한 인증으로, 해당 기업이 APEC 기준의 개인정보 보호 체계를 갖추었음을 각 국가의 인증기관으로부터 인정받는 방식이다. 이렇게 인증을 받은 개별 기업들은 APEC 내에서 개인정보를 자유로이 이전받을 수 있게 된다(다만, 각 국가별 법률에서 이를 국외이전의 법적 근거로 허용하여야 한다).

라. 표준계약조항(Standard Contractual Clauses, SCC)

표준계약조항은 GDPR 제46조 제2항 (c)호와 (d)호에서 그 예시를 찾아볼 수 있다. 즉, EU 집행위원회 또는 개별 국가에서 채택된 계약을 개인정보 제공자와 개인정보 수신인 사이에 체결하는 경우에는 개인정보의 국외이전을 허용하고 있다.

이러한 표준계약조항은 해당 개인정보의 수신인이 해당 개인정보를 EU 수준으로 보호하겠다는 점에 대해 계약상 의무를 부담하게 되는바, 정보주체의 권리가 보호될 수 있다는 점을 근거로 개인정보의 국외이전 근거로 사용되고 있다.

그리고 이러한 표준계약조항은 EU 이외에도 뉴질랜드, 아르헨티나 등에서도 개인정보 관련 법률에서 국외이전의 법적 근거로 도입을 하고 있다.

4. 현행 제도들에 대한 평가

개인정보의 국외이전 제도는 앞에서 설명한 정보주체, 기업 및 규제당국의 관심 사항들을 반영할 필요가 있다. 그러나 그 근간에는 개인정보를 이전받는 자, 즉 수신인이 개인정보와 정보주체의 권리를 충분히 보호한다는 신뢰에 기반을 둘 수밖에 없다.

그리고 위에서 언급한 제도들은 개인정보를 이전받는 기업의 개인정보 보호 수준 정도를 개인정보를 제공하는 기업 또는 정보주체가 거주하는 국가의 개인정보 보호 수준에 맞추도록 하는 제도로서, 개인정보 및 정보주체의 권리를 보호하는 방식이라는 점에서 동일한 방식으로 평가될 수 있다. 즉, 이러한 제도들은 국외이전을 위한 통로를 제공해 준다는 점에서 기업의 니즈를 충족시키면서도, 개인정보 및 정보주체의 권리를 보호할 수 있다는 점에서 각 당사자의 이익을 균형있게 조화시키는 방식으로 판단된다.

그러나 위에서 설명한 방식들은 개인정보 수신인의 개인정보 보호 정도에 대한 신뢰 구축 방식에 있어서는 차이점을 가지고 있다. 적정성 결정(또는 동등성 인정)과 기업에 대한 보호 수준 인증 제도는 개인정보를 이전받는 국가 또는 기업의 개인정보 보호 수준 정도를 규제기관에서 평가하여 그 평가에 따라 인증 등을 해 주는 방식으로 신뢰 부여의 주체가 정부 또는 규제기관이 되지만, 모델 계약조항은 국가나 기업의 보호 수준을 평가하는 방식이 아니라, 계약 조항을 통해 개인정보 수신인의 개인정보 보호 정도를 높이는 방식으로, 개인정보를 제공하는 자가 계약을 통해 신뢰를 구축한다는 점에서 그 차이를 가지고 있다고 볼 수 있다. 하지만 신뢰 구축을 통한 개인정보의 국외이전 허용이라는 점에서는 동등한 방식으로 평가될 수 있다.

디지털 경제의 발전에 따라 개인정보의 국외이전에 대한 니즈가 증가하고 있지만, 개인정보 보호의 관점에서 이를 무조건 허용해 줄 수 없다는 점은 모두가 인지하고 있는 사실이다. 그리고 이러한 점을 고려하여 개인정보의 이전에 대한 신뢰가 구축되어 있는 경우, 즉, 개인정보 보호 프레임워크가 적용될 수 있다는 믿음 하에서 개인정보 국외이전이 허용되어야 하므로, 이러한 점을 반영한 위와 같은 제도들과 그에 추가된 다른 제도들에 대한 고민도 필요하다고 할 것이다. 또한, 위 제도들이 전 세계적으로 도입되지 아니하고, 지역 단위로 도입되거나 국가 단위로 도입되고 있어 그 한계가 존재한다는 점도 분명하므로, CBPR 인증 제도의 확대(예를 들어, 글로벌 CBPR(Global Cross-Border Privacy Rules) 인증제도) 등 현행 제도들의 글로벌 차원으로 확대에 대한 전략적 논의가 필요한 점도 분명해 보인다.

5. 향후 우리가 고려하여야 할 사항 – 표준계약조항의 도입에 대한 검토 필요성

2023년 개인정보 보호법 개정으로 한국의 국외이전 매커니즘이 재정립된 것은 사실이다. 특히 개별 기업에 대한 인증 제도 및 국가에 대한 동등성 인정을 통해 개인정보의 국외이전의 편리성을 제고한 점은 주목할만한 성과라고 생각된다. 그러나 표준계약조항을 도입하지 않는 점에 대해서는 향후 재고의 여지가 있어 보인다. 표준계약조항의 경우에도 개별 계약을 통해 개인정보 수신인의 개인정보 보호 노력을 제고할 수 있다는 점에서 정보주체의 권리 등을 보장할 수 있는바, 이러한 제도를 도입하는 방안은 적극적으로 고려할 필요가 있다고 생각된다.

주석

[1] Autoriteit Persoonsgegevens, “Dutch DPA imposes a fine of 290 million euro on Uber because of transfers of drivers' data to the US”, 2024.8.26.

[2] ‘상호운용성(Interoperability)’이라는 용어는 소프트웨어 개발 부문에서 “기종이 다른 컴퓨터나 단말기를 연결하여 통신할 수 있으며 다른 기기의 이용자 간에 원활하게 정보를 교환하거나 일련의 처리를 수행할 수 있는 특성”이라는 의미로 주로 사용되었다.

[3] 영어 원문은 “Member countries should encourage and support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines”이다.

[4] OECD, “Report on the Implementation of the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data”, 2021.3.17. (URL: https://one.oecd.org/document/C(2021)42/en/pdf)

[5] ITIF, “How the G7 Can Use “Data Free Flow With Trust” to Build Global Data Governance”, 2023.7.27. (URL: https://itif.org/publications/2023/07/27/how-g7-can-use-data-free-flow-with-trust-to-build-global-data-governance/)

[6] G7/G20 Documents Data base, “G7 Digital and Tech Track Annex 1 – G7 Vision for Operationalising DFFT and Its Priorities”, 2023. (URL: https://g7g20-documents.org/database/document/2023-g7-japan-ministerial-meetings-ict-ministers-ministers-annex-g7-digital-and-tech-track-annex-1-g7-vision-for-operationalising-dfft-and-its-priorities)

[7] APEC(Asia-Pacific Economic Cooperation)은 아시아 태평양 지역 국가들 간의 경제적 협력을 강화하여 모든 회원국의 경제적 성장을 촉진하기 위한 지역 협력체이다. 그리고 APEC 프라이버시 프레임워크(Privacy Framework)는 개인정보의 적절한 보호를 통해 소비자의 신뢰를 제고하고, 이러한 신뢰를 기반으로 전자상거래를 촉진하고자 하는 목적으로 개인정보 보호를 위한 9개 원칙과 이러한 원칙의 이행을 위하여 필요한 사항을 규정하고 있다.

[8] ASEAN(Association of Southeast Asian Nations)은 동남아시아 국가들 간의 전반적인 상호협력을 증진하기 위한 지역 협력체이다. ASEAN은 2018년 디지털 데이터 거버넌스 프레임워크(ASEAN Framework on Digital Data Governance)를 발표하였고, 그

일환으로 2021년에는 국경 간 데이터 흐름을 위한 매커니즘으로 국경간 데이터 이전을 위한 모델 계약 조항을 발표하였다.

[9] GDPR Art. 45(1): “A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.”

[10] KISA, CBPR 소개 (URL: https://cbpr.kisa.or.kr/gdpr/static/cbpr_info.do)

참고 문헌

APEC(2019), APEC Steps Up Promotion of Cross-Border Privacy Rules

ASEAN(2016), ASEAN Framework on Personal Data Protection

ASEAN(2021), ASEAN Data Management Framework

OECD(2021), Interoperability of privacy and data protection frameworks

OECD(2023), Report on the implemenation of the recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data

Privacy Report
2024 개인정보 이슈
심층 분석 보고서

『Privacy Report 2024 개인정보 이슈 심층 분석 보고서』는
디지털·정보보호 관련 글로벌 트렌드
및 주요 이슈를 분석하여
정책 자료로 활용하기 위해 한국인터넷진흥원에서
기획, 발간하는 심층 보고서입니다.

본 보고서의 내용은
한국인터넷진흥원의 공식 견해가 아님을 알려드립니다.

발행

발행일 2024년 9월 30일

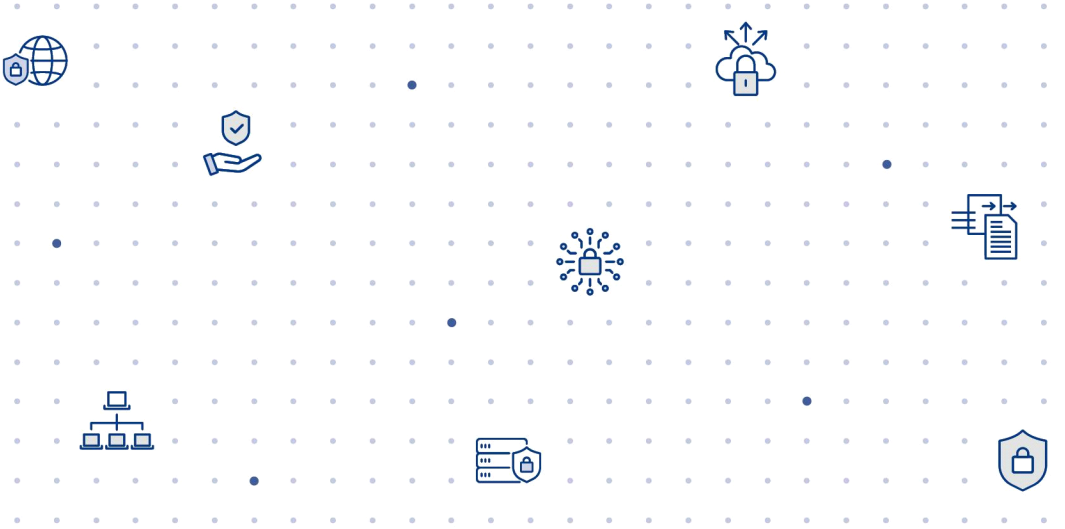
발행처 한국인터넷진흥원 개인정보제도팀
전라남도 나주시 진흥길 9
Tel : 061-820-1231

PRIVACY REPORT

2024 개인정보 이슈
심층 분석 보고서

2024 Vol. 4

PRIVACY REPORT



KISA 한국인터넷진흥원