Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.5, Oct. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.5.1205

유럽 PSD2 시행에 따른 금융분야 마이데이터 정책의 개인정보보호 강화 방안 연구

송 미 정,† 김 인 석‡
고려대학교 정보보호대학원

A Study on Privacy Protection in Financial Mydata Policy through Comparison of the EU's PSD2

Mi-Jung Song,† In-Seok Kim‡
Graduate School of Information Security, Korea University

요 약

데이터 기반 경제시대에서 데이터 활용능력이 경쟁력이 됨에 따라 개인정보의 보호와 더불어 개인정보의 활용을 통한 경제적 부가가치를 창출하려는 노력이 함께 강조되고 있다. 이 가운데 등장한 EU의 PSD2(the second Payment Service Directive)는 정보 주체의 '정보이동권'을 근거로 개인의 자기결정권을 보장하면서 데이터의 활용과 유통을 촉진하는 마이데이터 정책으로 전 세계 오픈뱅킹 정책의 시초가 되고 있다. 이러한 추세에 따라 우리나라 정부도 국내 금융업권별 실정을 반영하여 마이데이터 정책을 적극적으로 추진하고 있다. 하지만, 마이데이터 정책으로 인해 금융정보의 유통 및 활용 범위가 커진 만큼 개인정보의 유출 및 오남용, 해킹 등 위험도 커진 것도 사실이다. 본 연구에서는 EU PSD2가 어떻게 국내 금융분야 마이데이터 정책에 반영되어 추진되고 있는지를 살펴본다. 그리고 국내 마이데이터 정책의 개인정보보호 위험 사항을 개인정보 생명 주기별로 나누어 식별한 후 이러한 위험에 대한 법적 기술적 대응책을 제시하고자 한다.

ABSTRACT

As the ability to use data becomes competitive power in the data-driven economy, the effort to create economic value by using personal data is emphasized as much as to protect personal data. EU's PSD2(the second Payment Service directive) became the initiative of the Open Banking trends all over the world, as it is the Mydata policy which protects the data subject's right by empowering the subject to control over the personal data with the right to data portability and promotes personal data usages and transfer. Korean government is now fast adopting EU's PSD2 in financial sector, but there is growing concerns in personal data abuse and misuse, and data breach. This study analyzes domestic financial Mydata policy in comparison with EU's PSD2 and focus on Personal information life-cycle risks of financial Mydata policy. Some suggestions on how to promote personal information and privacy in domestic financial Mydata Policy will be given.
Keywords: PSD2, Open Banking, Mydata, Data Portability

Received(07. 30. 2019), Modified(09. 10. 2019), Accepted(09. 23. 2019)

† 주저자, mgjsong@gmail.com
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

I. 서 론

1.1 연구 배경과 목적

데이터가 모든 산업의 발전과 새로운 가치 창출의 촉매 역할을 하는 '데이터 기반 경제(data-driven economy)'시대가 도래하였다. '데이터 기반 경제'란 '데이터에 접근하고 활용할 수 있도록 협업하는 과정에서 데이터 생산, 인프라 제공, 연구조사, 데이터 소비 등 서로 다른 역할을 담당하는 구성원으로 이뤄진 생태계(ecosystem)'을 의미한다[1]. 데이터의 활용능력이 개인과 기업의 경쟁력 나아가 국가 경쟁력이 되는 시대이다. 세계 주요국은 데이터 경제 선도를 위해 범정부 차원에서 데이터 확보, 데이터 활용 확대, 데이터 분석 인재 양성 등과 함께 안전한 데이터 활용 제도 마련에 적극적이다[2]. 우리나라 역시 데이터 기반 국가 경쟁력 확보를 위해 데이터 경제 활성화 정책을 여러 방면에서 추진하고 있지만, 현실적으로 녹록지 않다[3]. 특히 데이터 중에서 가장 비중이 크고 활용가치가 크다는 개인정보는 헌법이 보장하는 개인의 사생활의 비밀과 자유와 밀접한 관련성을 가지는 만큼 그 활용에 더욱 민감하다.

과거 대량의 개인정보 유출 및 오남용 사고로 인한 개인정보 활용에 대한 국민적 우려와 불신이 팽배한 상태에서 현행 보호 위주의 엄격한 '활용 목적에 대한 사전 동의', '목적 외 활용 금지'의 개인정보보호법과 제도는 다양한 종류의 데이터가 융합되어 생성되고, 사람이 아닌 컴퓨터 알고리즘으로 대량의 데이터가 처리 및 활용되는 인공지능 시대의 데이터 활용을 가로막고 있다[4].

이러한 상황에서 IT산업에서 적용할 수 있는 개인정보보호 및 활용 정책으로 유럽을 중심으로 마이데이터(Mydata) 정책이 대안으로 제시되고 있다. 마이데이터란 기존 기업들이 보유하고 있는 개인정보에 대한 통제권을 해당 개인에게 돌려주고, 개인이 주체적으로 이를 관리·활용하도록 '데이터 이동권'을 보장하는 정책을 말한다. 마이데이터 정책은 개인정보의 주체적인 관리와 활용을 통해 개인의 합리적인 의사결정과 소비행태를 이끌어 내는 것은 물론 기업의 데이터 활용능력까지 제고[5]하는 동시에 특히 마이데이터 정책의 '데이터 이동권'은 융합 데이터 생태계를 촉진하면서 새로운 비즈니스 모델을 창출하고 지능화한 사회를 촉진할 것이다[6]. 특히 금융분야에 있어서 전 세계 오픈뱅킹(Open Banking)의 시초가 된 유럽의 PSD2를 참고해 세계 주요국에서는 금융분야 마이데이터 정책, 오픈뱅킹을 적극적으로 추진하고 있다.

우리나라 정부 역시 2018년 3월 19일 '금융분야 데이터 활용 및 정보보호 종합방안'을 발표하며 빅데이터·핀테크·사물인터넷·인공지능 등 4차산업혁명 시대에 맞는 금융분야 데이터 산업 활성화 및 경쟁력 제고에 적극적인 입장을 밝혔다[7]. 이어 2018년 7월 19일 '금융분야 마이데이터산업 도입방안'을 통하여 개인정보 자기결정권 보장, 금융소비자 보호 등을 위한 금융분야 마이데이터산업(이하 '본인신용정보관리업')의 도입과 신용정보법 개정안에 관한 구체적인 내용을 발표하였다[8].

정부의 이와 같은 금융분야 마이데이터 정책 및 관련 법 개정은 2018년 5월 25일부터 시행된 EU의 GDPR(General Data Protection Regulation)과 PSD2의 영향을 많이 받은 것으로 긍정적인 측면이 많지만, 금융 데이터의 이동성과 활용만을 강조한 나머지 성급하게 정책을 추진하게 되면 개인정보 유출 및 오남용, 해킹 등과 같은 사고가 발생할 수 있다. 따라서 정책의 추진과정에서 정보주체의 권리가 법적으로 보장되도록 관련 법과 제도를 정비하고, 개인의 프라이버시와 데이터가 안전하게 보호되고 활용될 수 있도록 기술 표준 및 관리 정책 마련이 선행되어야 한다.

본 연구에서는 국내 금융분야 마이데이터 정책의 주요 내용을 EU PSD2와 비교하여 살펴보고, 개인정보의 활용과 보호의 균형이라는 관점에서 현재 마이데이터 정책 추진 내용의 개인정보보호 강화를 위한 기술적 제도적 제언을 하고자 한다.

1.2 연구 방법 및 구성

본 연구는 EU PSD2 및 국내 금융분야 마이데이터 정책, 오픈뱅킹 제도 등과 개인정보보호와 활용관련 국내외 문헌들을 수집하여 분석하는 문헌 연구방식으로 이루어졌다. 본 연구의 구성은 다음과 같다. 제1장은 연구의 필요성과 목적 및 방법 및 구성에 대해 다룬 서론 부분이며, 제2장은 연구의 이해를 돕기 위해 정보이동권과 마이데이터 정책, 금융분야 마이데이터 정책의 의의와 효과, 해외 마이데이터 정책 사례를 다룬다. 그리고 관련된 선행 연구를 다루었다. 본론에 해당하는 제3장은 EU PSD2와 국내 금융분야 마이데이터 정책의 주요 내용을 비교하며

살펴본다. 제4장은 마이데이터 정책의 프라이버시 및 보안 이슈를 개인정보 생명주기 단계별로 분석해 보고 제5장은 마이데이터 정책의 프라이버시 및 보안 강화 방안들을 살펴본다. 마지막으로 제6장은 결론과 제언으로 마무리한다.

II. 이론적 배경

2.1 정보이동권과 마이데이터 정책

GDPR 제20조에 따르면 '정보이동권'이란 '정보주체자의 요청에 따라 컨트롤러에게 제공한 자신의 정보를 통상적으로 사용되고 기계로 판독 가능한 형식으로 받을 수 있는 권리를 말하며, 기술적으로 가능한 경우에는 정보주체자의 개인정보를 직접 다른 컨트롤러에게 이전할 수 있는 권리'로 명시하고 있다[9]. EU GDPR의 '정보이동권' 등장 배경에는 구글, 페이스북, 애플, 아마존과 같은 미국 IT 플랫폼 기업들의 시장 지배에 대한 경계심이 있었다. 이들 거대 IT기업에 대한 데이터 시장 탈환 무기로 정보이동권을 들고 나온 것이다. 즉 정보주체가 자신의 정보가 쌓여있는 거대 IT 플랫폼 기업에게 고착화(lock-in)되는 것을 피해 더 나은 서비스 제공자를 찾아서 경쟁관계에 있는 다른 정보처리자에게 이전할 수 있도록 해줌으로 소비자의 선택권 확대와 함께 구글, 페이스북, 아마존과 같은 거대 플랫폼 기업의 데이터 시장 지배를 경계한다는 것이다.

이렇게 등장한 정보주체의 정보이동권이 빅데이터 시대에 개인정보 활용 서비스에 대한 기존 규제에 대한 패러다임 변화라는 관점에서 주목받고 있다[10]. 특히 정보이동권을 근거로 기존 기업들이 보유하고 있는 개인정보에 대한 통제권을 정보주체인 개인에게 돌려주고, 정보주체자가 여러 기업들에 흩어져있는 자신의 데이터를 모아 주도적으로 활용하고 관리하도록 하는 '마이데이터 정책'이 개인정보 보호와 활용 사이의 균형을 이룬 정책으로 주목받게 된 것이다.

2.2 금융분야 마이데이터 정책의 의의와 효과

금융산업은 그 발전과정에서 여신심사 등에 다양한 데이터를 활용하고 신용정보 집중제도 등을 통해 관련 정보를 집중하는 한편, 은행・카드・보험・증권 등 금융업권별로 체계적으로 관리되고 정형화된 데이터가 대량으로 축적되어 있다. 또한 금융 데이터는 정확도도 매우 높고 정보통신・유통・의료 등의 타 산업과의 융합이 용이하여 데이터의 경제적 가치가 매우 높다. 금융분야 마이데이터 정책은 정보주체인 개인의 동의하에 금융기관 뿐만 아니라 혁신적인 서비스를 제공하는 핀테크 회사 등에 본인의 금융데이터에 대한 다양한 접근과 활용을 보장함으로 기존에는 제공할 수 없었던 통합계좌정보조회, 맞춤형 금융상품 등의 새로운 서비스를 가능하게 해준다. 이를 통해 소비자 개인이 합리적인 의사결정을 통해 경제적으로 직접적인 이익을 얻게 될 뿐만 아니라 금융산업 전반에 걸쳐 혁신과 변화가 야기될 것이다.

금융분야 마이데이터 정책이 가져올 변화들을 살펴보면 첫 번째는 기존 대형 은행들의 독점적 위치가 사라지고 금융산업내 경쟁 심화를 들 수 있다. 이러한 금융산업내 경쟁촉진은 소비자에게 더 많은 혜택을 줄 것이다. 은행, 신용카드, 증권회사, 보험회사 등 금융기관들에 흩어져 있는 개인의 계좌정보, 카드정보 및 지출내역, 보험 가입 내역 등을 통합조회하고, 각종 금융상품들을 한눈에 비교 분석하는 것이 가능해지면 소비자는 더 현명해지고, 이제는 금융기관의 인지도나 주거래은행이라서 상품을 가입하는 것이 아니라 제공받는 금융상품과 서비스 자체로 평가하게 될 것이다. 둘째로 금융기관 및 핀테크 회사들이 개인별 맞춤형 상품 및 서비스를 개발하고 제공하는 것이 가능해지는 것이다. 기존에는 업종내 또는 기관내 보유하고 있는 고객 데이터만을 기반으로 금융상품을 개발하고 신용등급을 판단할 수 밖에 없었지만 마이데이터를 통해서 고객의 종합적인 재무 상태나 소비습관, 위험성향 등에 대한 분석이 가능해지면서 보다 정교한 개인별 맞춤형 상품을 개발 및 제공이 가능해질 것이다. 마지막으로 금융산업의 디지털 혁신을 가속화할 것이다. 마이데이터 정책의 각종 서비스는 온라인 채널을 통해 제공되기 때문에 기존 금융기관들의 디지털 뱅크로의 변화가 가속화될 것이다. 이 과정에서 오프라인 지점 및 대규모 창구 인력 축소에 따른 금융산업 전체의 비용 절감 및 효율성 증대 효과가 나타나겠지만 한편으론 이러한 디지털 혁신이 비대면 채널에 익숙한 젊은 층에게는 활발하게 쓰이는 반면 IT기기에 익숙하지 않은 고령층을 소외시키는 디지털 세대격차를 심화시킬 우려도 존재한다[11].

2.3 해외 정책 사례

EU PSD2 시행에 따라 영국 경쟁당국(Competition & Market Authority, CMA)에서는 'Retail Banking Market Investigation Order 2017'를 발표하고 2018년 1월 13일부터 'Open Banking Standards'라는 정책을 시행하였다. 이미 2011년 4월부터 영국 정부는 자국내 모든 산업에 걸쳐 적용되는 마이데이터 원칙을 발표한 바 있으며, 2015년 3월 재무부에서 은행API공개의 필요성을 언급하며 그 후속 조치로 2015년 9월 업체 및 데이터 전문가와 시민단체, 기업 등이 참여하는 Open Banking Working Goup(OBWG)이 결성되어 오픈뱅킹의 표준을 수립하는 작업을 착수하였다.

그리고 2018년 9월 7일 영국의 OBIE(Open Banking Implementation Entity)는 표준 API 요건을 담은 'Open Banking Standards ver3.0'를 발표한다. 오픈뱅킹 정책에 따라 영국 내의 9개 대형 은행들(CMA9)은 고객이 원할 시에 해당 고객의 금융거래정보를 오픈API를 통해서 제3자 서비스제공업자(Third-Party Provider) 의무적으로 제공해야 한다. 영국 오픈뱅킹의 특징은 금융기관이 고객의 계좌정보 뿐 아니라 금융상품의 정보까지 제3자에게 API로 공개토록 의무화한 것이다[12]. 즉 PSD2에서 요구하는 고객 지급결제계좌관련 정보뿐 아니라 은행에서 판매하고 있는 개인과 기업의 계좌 상품정보까지 제공하도록 하여 소비자인 개인이 여러 금융회사의 다양한 상품정보를 한눈에 비교하여 합리적인 의사결정을 할 수 있도록 하고 있다.

호주 정부 역시 은행이 보유한 데이터의 전면 개방을 추구하는 가운데 은행이 공개해야 할 금융상품의 범위가 EU나 영국에 비해 훨씬 넓다. 호주 재무부는 단계적인 오픈뱅킹 정책을 추진을 통해 2019년 7월부터는 거래계좌, 신용 및 직불카드, 예금, 외화 등의 상품정보를 공개하고, 2020년 2월부터는 담보대출, 개인대출, 사업대출 상품정보를 의무적으로 제공토록 할 예정이다.

일본은 2017년 2월 은행법 개정을 통해 은행에 데이터 및 지급결제시스템 개방에 필요한 Open API를 구축할 노력 의무를 부과하였고, 미츠비시 UFJ, 미츠이 스미토모, 미츠호 등 주요은행이 Open API를 제공하고 있으며, 2020년까지 80개 은행이 Open API를 구축하여 제공할 것을 목표로 하고 있다.

2.4 선행 연구

EU GDPR의 시행 이후로 정보주체의 권리 보장을 통한 개인정보 보호 및 활용 제도에 대한 연구가 활발히 이루어지고 있는 가운데 박훤일(2017)은 GDPR의 정보이동권의 국내 도입의 필요성을 주장하며 정보통신망법과 신용정보법에 근거규정을 마련할 필요가 있다고 보았다[10]. 조수영(2018)은 EU의 GDPR의 정보주체의 기본권 보장을 위한 '개인정보의 이동권(right to data portability), 처리제한에 대한 권리, 반대할 권리, 자동화된 결정 및 프로파일링관련 권리' 등의 우리나라 법제에 맞는 도입과 현행 개인정보영향평가(PIA)의 개선을 주장하였다[13]. 하지만 EU PSD2 등장으로 정부가 적극적으로 추진하고 있는 금융분야 마이데이터 정책들에 대한 종합적인 분석 및 개인정보보호와 활용에 대한 연구는 아직 없었다. 따라서 본 연구는 유럽 PSD2가 국내 금융분야 마이데이터 정책에 어떻게 반영되고 있는 지를 비교하여 살펴보고, 개인정보보호의 관점에서 개인정보 생명주기 단계별로 마이데이터 정책의 프라이버시 및 보안 위험들을 식별 이에 대한 법적 제도적 방안에 대해 제언을 하고자 한다.

III. EU PSD2와 국내 금융분야 정책

3.1 EU PSD2의 주요 내용

유럽연합(EU)은 EU내 통합된 지급결제 시장을 형성하고 소비자를 보호하기 위해 2007년 12월 PSD(Payment Service Directive)를 제정하여 운영해왔다. 하지만 기존에는 대상 범위가 은행으로 한정되어 있어 최근 급격하게 증가한 온라인 및 모바일 지급결제서비스를 제공하는 핀테크 및 IT 업체들을 규제 대상으로 포함시키기 위해 2015년 12월 개정된 PSD2(The Revised Payment Service Directive)를 발표하고, 2018년 1월 13일부터 시행하였다.

PSD2의 목적은 신생 핀테크 업체들을 포함한 금융 서비스 제공자들에게 공평한 경쟁 환경을 제공하여, 보다 효율적이고 통합된 온라인 지급결제서비스 시장을 형성하고 동시에 소비자 데이터 보호 및 보안을 강화하는 데 있다[14]. 특히 PSD2는 핀테크 업

체 등의 제3자 지급결제서비스 제공업자(Third Party Payment Service Provider, TPP)들이 통합계좌정보서비스를 제공하거나 지급결제서비스 인프라를 구축할 수 있도록 은행 등의 계좌정보제공자(Account Servicing Payment Service Provider, ASPSP)가 오픈 API 등과 같은 인터페이스를 통해 고객 계좌정보에 대한 액세스 권한을 제공하는 것을 의무화하고 있다. 전 세계 '오픈뱅킹(Open Banking)'의 시초가 된 이 새로운 금융 산업 규제는 전통적인 금융기관이 기득권을 가지고 지배하던 금융데이터를 개방하여 소비자의 자기결정권 강화 및 합리적 의사결정을 돕는 것은 물론 금융산업의 경쟁력 제고 및 지급결제시장의 혁신의 시초이다.

Fig.1 과 같이 PSD2에서 새롭게 도입된 TPP는 기능상 크게 2가지 유형으로 나누어 서비스 범위 및 권한 등을 명시되어 있다.

첫 번째 유형은 계좌정보서비스제공업자(Account Information Service Provider, AISP)이다. AISP는 은행 등 여러 금융기관에 분산되어 있는 고객의 결제계좌 관련 정보를 통합하여 조회하도록 하는 온라인 서비스를 제공한다. 여러 금융기관에 분산되어 있는 사용자의 결제계좌정보들을 통합 조회하는 서비스를 비롯해 다양한 데이터 연계를 통한 분석 서비스 및 고객 맞춤형 서비스 등이 AISP의 서비스 범주에 포함된다. 예를 들어, 고객의 지출내역을 통합하여 소비습관을 분석해주거나, 고객 자산, 대출, 지출관

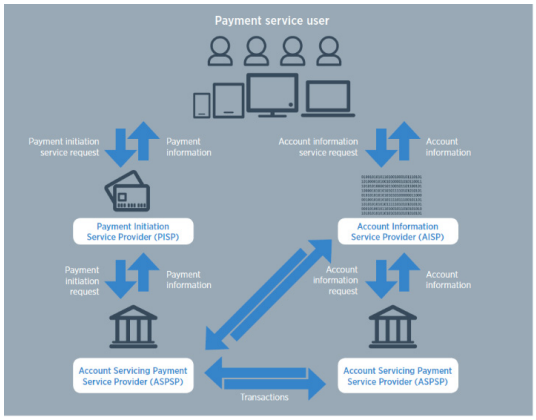


Fig. 1. The new service providers introduced by PSD2 [15]

련 데이터들을 신용정보회사나 재무 컨설팅 회사 등에 제공해서 신용등급관리 서비스 및 맞춤형 자문서비스 등을 제공할 수 있다.

두 번째 유형은 지급지시제공업자(Payment Initiation Service Provider, PISP)이다. 이들은 온라인 상거래상 사용자의 요청에 따라 지불계좌와 관련하여 지급 거래를 개시하는 서비스를 제공한다. PISP는 사용자의 지불계좌 정보에 대한 접근은 하지만, 지급인과 수취인 계좌 간의 지급지시를 통한 대금결제 기능만 수행한다. 은행으로부터 대금을 지급 받아 보유하거나 잔액 정보 등 계좌정보를 열람할 수 있는 권한은 없다.

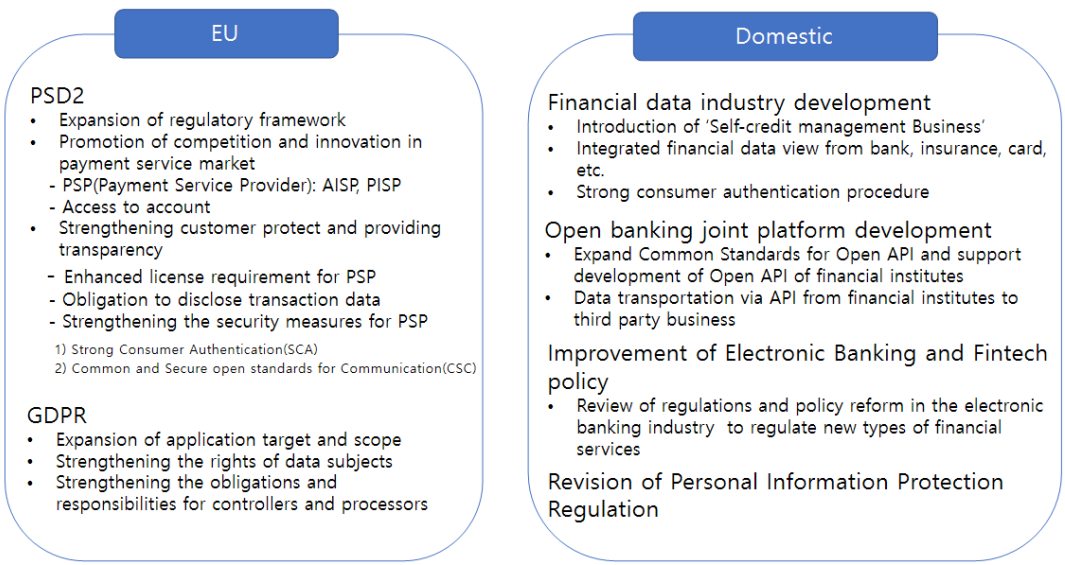


Fig. 2. Comparison between EU and Domestic Financial MyData Policy[16]

3.2 국내 마이데이터 정책의 주요 내용

EU PSD2의 영향을 받아 우리나라 정부도 데이터 산업, 핀테크 및 전자금융 분야에 걸쳐 적극적으로 정책을 추진하고 있다. 단 국내의 경우 전자금융 관련 산업과 법제도가 세분화되어 있어, 이에 대해 마이데이터 정책 역시 훨씬 더 광범위하고 제공 방식 및 서비스 기술 규제 조건도 상세하게 명시하고 있다.

Fig.2.에서는 EU와 국내의 금융분야 마이데이터 정책의 주요 내용을 비교하고 있다. 즉, EU의 PSD2가 온라인 지급결제시장을 중심으로 API를 통한 계좌정보 및 지급결제서비스 중심의 정책인 반면 국내의 금융분야 마이데이터 정책은 1)은행의 계좌정보 뿐만 아니라 보험, 증권, 카드 등 전 금융영역의 데이터를 포함하여 통합하여 조회할 수 있도록 '본인신용정보관리업'을 신설하고, 지급결제분야와 관련해서도 정부가 적극적으로 개입하여 2)금융결제원의 '온행권 공동 오픈플랫폼 개발 사업'을 통한 핀테크업 활성화 정책 및 3)핀테크 관련 법 개정을 통한 지급지시업 및 종합결제업 등을 도입하는 등 데이터 산업, 핀테크업 및 오픈뱅킹플랫폼 구축 등 훨씬 더 광범위하다.

3.2.1 '본인신용정보관리업' 도입

2018년 7월 금융위원회는 금융소비자 주도의 금융혁신을 위해 소비자의 신용·자산·정보관리 등을 도와주는 '금융분야 마이데이터(MyData)산업 도입 방안'을 발표하였다[8]. 특히 해외 주요국에 비해 저조한 금융분야 데이터 사업을 육성하고자 신용정보법 개정을 통해 개인신용정보 이동권을 우선 도입하고 '본인신용정보관리업'을 신설하여 인가받은 업자가 신용정보통합조회 서비스와 계좌정보업무, 데이터 분석 및 컨설팅, 투자자문, 금융상품 자문 등을 수행할 수 있도록 하였다. 특히 정보주체의 명시적 동의(informed consent)에 기반하여 본인정보를 보유한 금융회사로부터 개인(신용)정보를 전산상으로 제공받아 본인에게 통합조회 서비스를 제공한다는 부분에서 EU PSD2의 AISP와 동일하지만, 그 대상이 은행·상호금융·저축은행·보험사 등의 예금계좌 입출금 내역, 신용카드·직불카드 거래내역, 대출금 계좌정보, 보험계약 정보와 증권사의 투자자예탁금·CMA 등 다양한 계좌의 입출금 내역 및 금융투자상품(주식·펀드·ELS 등)의 종류별 총액정보, 전기통신사업자의 통신료 납부내역 등의 신용정보를 포함하고 있다. 따라서 은행 뿐만 아니라 카드회사, 보험사, 증권회사, 전기통신사업자까지 그 정보제공대상 기관의 범위가 역시 훨씬 광범위하다.

3.2.2 은행권 공동 오픈플랫폼 개발 사업

사실 우리나라 정부는 핀테크 산업 육성 초기부터 핀테크 인프라 구축을 위해서 힘써왔다. 2015년 7월 '금융권 공동 핀테크 오픈플랫폼' 정책을 발표하고, 핀테크 기업과 금융회사간의 협업을 도모하였다. 2016년 8월 세계 최초로 금융결제원과 코스콤을 중심으로 오픈API 방식의 '금융권 공동 핀테크 오픈플랫폼'을 구축하여, 계좌 및 잔액 조회뿐 아니라 이체, 주식주문 등과 같은 다양한 기능을 제공하였다. 하지만, 모든 금융기관에 해당 정책을 의무화할 법적 근거가 없어서 서비스 내용에 한계가 존재하였고. 현실적으로도 금융결제원의 전산망의 수용 능력이 크지 않아 많은 핀테크 회사들의 트래픽을 감당할 수 없었다. 또한 핀테크 업체에게만 과도하게 높은 수수료를 부과하는 등의 문제도 있었다.

그 후 2019년 2월 관계부처 합동으로 기존 '은행권 공동 오픈플랫폼'을 전면 개편하는 핀테크 및 금융플랫폼 활성화를 위한 '금융결제 인프라 혁신 방안'을 발표하고 모든 참여자들이 합리적인 비용으로 이용할 수 있도록 금융결제원의 인프라를 업그레이드하여 핀테크회사에 개방한다고 밝혔다[17]. 1단계로 핀테크 회사의 트래픽을 감당할 수 있을 만큼 금융결제원의 시스템을 증설하고 핀테크 회사에 건당 400~500원 부과하던 수수료도 현행 대비 1/10로 낮춘다는 계획이다. 2단계로는 전자금융거래법 개정을 통해 핀테크 회사가 차별 없이 은행결제망을 이용할 수 있도록 오픈뱅킹을 법제도화 한다는 방침이다. 모든 은행들이 표준API를 통해 핀테크 회사에 이체 기능을 제공하도록 의무화하고, 해당 API를 통해 들어오는 거래에 대해서 처리순서, 처리시간, 비용 등에서 차별을 금지한다는 내용도 포함시킬 예정이라고도 밝혔다. 이와 같은 내용은 EU PSD2의 ASPSP의 오픈API 제공 의무 및 차별금지 조항을 참고한 것으로 보인다. 3단계 중장기적으로는 일정한 자격을 갖춘 핀테크 결제 사업자가 금융결제망에 직접 참가하여 독자적으로 자금이체를 할 수 있도록 제도를 마련할 예정이다.

3.2.3 전자금융업 관련 체계 및 규제 개혁

현재의 국내 핀테크 관련 규제는 업종별, 서비스 영역별로 진입 규제를 적용함에 따라 융합·복합 서비스 제공시 각각의 라이센스를 획득해야 하고, 유사한 기능을 가진 결제수단을 달리 취급함에 따른 규제 차이, 공백의 문제가 발생하였다. Table.1 의 국내 핀테크 관련 규제 법률에서 보듯이 업종별 가능한 서비스 범위 및 영역을 열거하는 positive 방식의 법 규제로 인해 새로운 서비스나 기술 등장에 적시에 대응하지 못하는 한계가 있었다.

정부는 이와 같은 체계를 기능별 규율 체계로 전환하여 새로운 기술과 서비스를 유연하게 포괄할 수 있도록 탄력적 규율 체계로 전환한다는 방침이다. 이러한 탄력적 규율 체계로 전환을 통하여 PSD2의 PISP와 같이 결제자금을 보유하지 않고 정보만으로 결제서비스를 제공하는 '마이페이먼트(My Payment)'을 도입하여 지급지시서비스에 한번의 로그인만으로 모든 은행의 자기 계좌에서 결제 및 송금 처리가 될 수 있도록 하고, '종합지급결제업'의 도입을 통해 은행과의 제휴없이 독립적으로 계좌를 발급·관리하고, 이를 통해 자금이체를 할 수 있도록 할 예정이다.

Table. 1 Fintech Business-Related Regulatory Laws[20]

Business Domain	Related Laws
Electronic Finance Business (e-payment, e-transfer)	Electronic Financial Transactions Act
Electronic Finance Assistant Business(VAN, ATM, etc)	Electronic Financial Transactions Act
Digital Bank	Banking Act
Crowd funding, Robo-Advisory	Financial Investment Services and Capital Markets Act
Online Insurance tech	Insurance Business Act
Customer Big data Analysis	Credit Information Use and Protection Act, Personal Information Protection Act
New Financial tech (security and online authentication tech)	Electronic Financial Transactions Act
P2P loan	- (Guidline)

IV. 마이데이터 정책의 개인정보 생명주기별 프라이버시 및 보안 이슈

앞에서 살펴본 정부의 적극적인 금융분야 마이데이터 정책은 금융분야 데이터 산업 활성화 및 서비스 혁신에 매우 긍정적으로 작용할 것이다. 하지만 개인정보 유출·노출·오용·남용 등 다양한 프라이버시 위험과 데이터 보안의 위험이 커진 것도 사실이다. 특히 데이터의 이동으로 인해 수집되는 정보의 범위가 확대되고, 금융정보가 다른 개인정보들과 융합·연동되어 민감 정보가 유출됨으로 프라이버시를 침해할 가능성이 커졌다. 또한 소비자의 재산과 직접적으로 연관되는 금융 데이터가 금융회사에서 핀테크회사로 이동함에 따른 데이터 보호와 보안 리스크도 커진 것도 사실이다.

본 장에서는 마이데이터 프로세스에 맞게 개인정보 생명주기별로 프라이버시 및 보안 위험 요소를 분석해보고자 한다. Table.2.와 같이 크게 수집, 이용과 제공, 그리고 저장과 파기 3가지로 나누어 프라이버시 및 보안 위험 요소를 분석해본다.

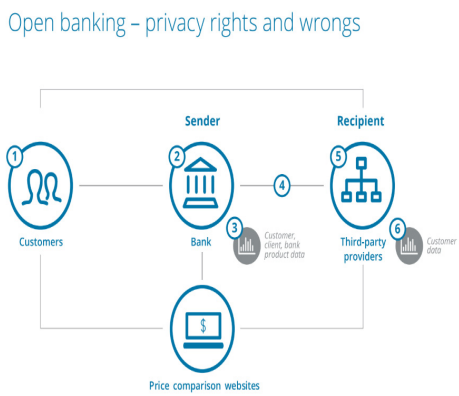
4.1 데이터 수집: 동의 관련 위험

마이데이터는 기존에 개인정보를 보유한 기관들로부터 개인정보를 전송 받아 이를 통합·연결한 후 맞춤형 금융서비스 등을 위해 이용하는 것이다. 따라서 마이데이터 프로세스의 시작은 정보주체의 '동의'로부터 시작된다. 수집단계에서 나타날 수 있는 개인정보 보호 위험요소들은 다음과 같다.

- 동의 없는 개인정보 수집
- 동의 및 고지 없는 개인정보 정보주체 외로부터의 수집
- 기망에 의한 개인정보의 수집
- 금융정보 관련자들의 동의 없는 정보 수집

즉 마이데이터 사업자는 정보주체로부터 동의를 받아 개인정보를 대리 수집하는 것이기 때문에 수집단계의 위험은 거의 동의와 관련된 부분이다. 하지만 현행 국내 법령상 동의 제도는 지나치게 복잡하고, 사용 목적 등의 방대한 고지사항을 하나하나 나열하도록 하고 있어 오히려 개인들에게 피로감(fatigue)만 유발할 뿐 정보주체가 고지사항에 대해 제대로 인식하지 못한 상태로 형식적으로 동의가 이루지고 있는 상황이다. 형식적인 동의 문제뿐만 아니라 마이데

Table 2. Data Sharing Steps and Risks(18)



life cycle	What needs to occur	Risks: What could go wrong
Data collect	① The customer initiates the data sharing request	The consent provided is incomplete and does not include all parties to an account
		The customer data sharing request is forged
	② The data sender ensures that the have an express consent which specifies what data is shared, clear purpose, who it is shared, which facilitates transparency	Express consent is not received
		The consent received is incomplete and does not includes all parties to an account
		The data sender failed to accurately record what data is to be shared, for what purpose, who it is to be shared with or for how long.
		The data sender fails to satisfy accreditation requirements
Data use and transfer	③ The data sender ensures they are able to identify and correctly extract only the customer data that they have consented to share and the data is secure	The wrong data for a customer is extracted
		The wrong customer's data is extracted
		The data holder fails to protect the data held
	④ The data transfer occurs in the correct format in a secure environment	The wrong data is transfered
		The data is transfered to the wrong party
		A data breach occurs during the data transfer
Data save and disposal	⑤ The data recipient confirms that they have express consent which prescribed the specific purpose the data can be used for and how long the data is to be held	The data recipient fails to receive express consent for the data use
		The data recipient fails to record the specific purpose for which the data can be used
		The data recipient fails to record how long the data is to be held
		The data recipient fails to satisfy accreditation requirements
	⑥ The data recipient ensured they are able to identify and use the data only for the purpose for which the customer has given consent and the data is secure	The data recipient uses the data for an inappropriate purpose for which they have not received consent
		The data recipient retains the data for a loner period than that for which have consent
		The data recipient fails to protect the data received

이터 사업에서는 전송 데이터 범위와 데이터 전송 상대자에 대해 정보주체의 통제 문제가 발생할 수 있다. 정보주체자인 개인이 본인의 정보 중 어느 정보까지, 어느 기관까지, 어떤 목적으로 정보를 제공할 것이지를 결정할 수 있고 해당 내용이 제대로 반영되어야 하지만 이같이 내용이 제대로 구현될 수 있을지 의문이다.

그 외에 계좌관련 정보에는 실제 동의를 한 정보주체 외에도 관련된 다른 사람들의 정보까지 노출되는 프라이버시 문제가 발생할 수 있다.

현재까지 EU 및 국내에서는 침묵하는 당사자(silent party)의 문제를 크게 보고 잊시 않지만, 대량의 데이터가 축적되어 융합 및 활용되면 또 다른 프라이버시 침해 문제가 될 소지가 있다.

4.2 데이터 이용과 제공: 제공방식의 위험

데이터 전송요청을 받는 금융기관 등은 안전하고 보안이 적용된 방식으로 정확한 데이터를 핀테크업자 등에게 제공해야 한다. 특히 금융기관 등 데이터를 제공하는 단계에서 발생할 수 있는 리스크는 다음과 같다.

- 동의 없는 개인정보의 무단 제공
- 다른 사람의 정보 제공
- 서비스 목적 달성과 관련 없는 과도한 개인정보 제공
- 제공 과정에서 외부인의 불법적 접근으로 인한 개인정보 유출 및 훼손, 변경
- 전송되는 정보 내역 미기록
- 중요정보 및 민감정보 전송

특히 마이데이터 정책을 통해 금융데이터가 A기관에서 B기관으로 이동하기 때문에 안전하고 보안이 적용된 전송방식에 대해 논란이 많다. 현재 계좌통합조회 서비스를 제공하는 주요 핀테크회사들은 Screen Scraping 방식을 많이 사용하고 있다. Table.3.과 같이 Screen Scraping 방식은 업체가 고객에게 개별 금융기관의 아이디와 비밀번호 또는 공인인증서를 입력 받아 금융기관의 웹사이트에 대리 접속하여 고객 데이터를 수집하는 방식으로 금융기관의 명시적 허가 없이도 업체가 고객을 대신하여 데이터를 수집할 수 있다. 하지만 보안에 취약하고 사고 위험이 대단히 높다.

첫째로 중요 인증정보(ID/PW)를 핀테크 업체 서비스에 입력·저장하여 해킹시 중요정보가 유출될 가능성이 있고, 둘째로 해당 업체가 고객 제공 서비스에 필요한 이상의 정보에 접근 가능하여 이용자의 개인정보에 대한 오·남용과 악의적 활용 가능성이 높다. 셋째로 서비스 탈퇴시에도 입력한 인증정보를 모두 변경하거나 인증서를 재발급해야하는 번거로움이 발생하고 미변경시에는 2차 유출 피해가 발생할 우려가 있다. 마지막으로 금융기관과 협의하여 별도의 보안 대책이나 보안 기술을 적용하기 힘들고, 웹사이트 출력 환경 변경에 따른 지속적인 관리가 필요하다.

Table 3. Screen Scraping vs. API

Screen Scraping	API
Direct access with credentials transfer	Interface access, no credentials transfer
Data (including user's credentials) breach risk when hacked	Token disposal and token access control when hacked
Excessive access to Data than necessary Data abuse and misuse risk	Easy to control the data access within the range to which the user consented
Hard to apply separate data protection or security technology	Possible to apply separate data protection technology with banks' support

4.3 데이터 저장과 파기: 관리의 위험

데이터 수신자인 마이데이터 사업자는 정보주체인 개인이 동의한 서비스 목적을 위해서 데이터를 안전하게 저장하여 관리하고, 동의한 기간이 지나거나 제공 동의를 철회한 경우 즉시 파기해야 한다. 저장과 관리, 파기 단계에서 발생할 수 있는 리스크는 다음과 같다.

- 정보처리자에 의한 개인정보의 유출, 훼손, 변경
- 불법적 접근에 의한 개인정보의 유출, 훼손, 변경
- 기술적 관리적 미비로 인한 개인정보의 유출
- 고객의 개인정보 동의 철회나 삭제 요구에 불응
- 보유 기간 지난 개인정보의 미파기

대량의 개인정보를 취급하게 되는 마이데이터 사업자에 대한 주기적인 관리·감독이 필요한 부분이다. 이 부분에 대해서는 아래에서 자세히 논의하도록 한다.

V. 마이데이터 정책의 프라이버시 보호 및 보안 강화 방안

앞에서 살펴본 바와 같이 마이데이터 정책은 개인정보 활용면에서는 분명 긍정적인 효과가 있지만, 개인정보 보호 및 보안 측면에서는 해결할 과제가 많다. 이를 해결하기 위해 유럽 및 우리나라 정부는 여러 가지 법적 제도적 장치를 마련하고 있다.

EU의 EBA(European Banking Authority)는 모든 PSP가 지켜야 할 규제적 기술 기준인 RTS(Regulatory Technical Standards)를 2018년 3월 13일 작성하여, 2019년 9월 14일부터 시행에 들어간다. RTS에는 SCA(Strong Customer Authentication)과 CSC(Common and Secure open standards for Communication)의 내용을 포함하여 PSD2의 소비자 보호 및 보안에 대한 기술적 규제 기준을 제시하고 있다[20]. EU의 GDPR 또한 개인정보보호를 위한 정보주체의 권리들을 법적으로 명시하고, 개인정보의 처리가 GDPR에 준수하여 수행되는 것을 보장하기 위해 처리보안 등 적절한 기술적 조직적 조치를 위할 의무 외에 책임성 강화를 위해 설계 및 기본 설정을 통한 정보보호(data protection by design and by default) 이행, 처리활동의 기록, 높은 위험(high risk)을 내재한 개인정보 처리에 대하여 개인정보 영향평가 수행, DPO(Data Protection Officer)의 지정, 개인정보 침해 통지 등의 정보처리자의 의무를 명시해놓고 있다. 이러한 EU의 프라이버시 및 보안 강화 제도들을 참고하여 국내 환경에 맞게 필요한 조치를 취할 필요가 있다.

5.1 수집단계: 정보주체의 권리 보장과 동의 규제의 합리화

5.1.1 정보주체의 권리 보장

개인정보는 개인의 사생활 비밀과 자유와 밀접한 관련성을 가지는 만큼 개인정보에 관한 정보주체의 정당한 권리와 이익을 충분히 보장하는 것을 선결 과제로 삼아 추진해야 할 필요가 있다. 특히 법률이 보호해야 할 대상이 되는 정보주체의 권리를 보다 명확하게 규정하여 급격한 기술 발전과 사회 변화를 고려하여 다양한 측면에서 정보주체의 권리 강화를 도모해야 한다. 이런 점에서 EU GDPR에서 규정하고 있는 다양한 정보주체의 권리들에 대해 분석해보고 국내법에 명시되어 있지 않는 정보주체의 권리에 대해 우리나라 법률체계에 맞게 반영할 필요가 있다.

특히 마이데이터 정책과 관련하여 누락된 정보주체의 '정보이동권'은 정보주체가 특정 금융기관에 종속되지 않고, 본인이 더 편리하고 이익되는 상품과 서비스를 선택할 수 있도록 보장해줌으로써 정보주체의 자기결정권을 강화해주기 때문에 법률로써의 도입이 필요하다. 신용정보법 개정안 제33조의2 '신용정보전송권'으로 "개인인 신용정보주체는 대통령으로 정하는 신용정보 제공 이용자나 개인정보보호법에 따른 공공기관에 대하여 그가 보유하고 있는 본인에 관한 개인신용정보를 다음 각 호의 어느 하나에 해당하는 자에게 전송하여 줄 것을 요구할 수 있다"고 반영되어 있지만 그 범위가 한정적이므로, 개인정보 보호에 관한 기본법인 개인정보 보호법 개정안에 반영되어 정보주체의 권리를 보장하고 대상 정보의 범위를 확장할 필요가 있다.

5.1.2 동의 제도의 합리화

개인의 개인정보자기결정권(자신에 관한 정보가 언제, 누구에게, 어느 범위까지 알려지고 또 이용되도록 할 것인지를 정보주체 스스로 결정할 수 있는 권리)[19]를 구현하기 위한 기본 수단은 '동의 제도'이다. 이러한 동의제도가 지금과 같이 형식적으로 계속된다면 정보주체의 개인정보자기결정권 행사가 실질적으로 보장된다고 볼 수 없다.

개인정보 수집단계에서 정보주체의 개인정보 자기결정권 행사에 있어서의 '형식적 동의' 문제를 인식한 EU은 PSP의 개인정보 접근에 대해서 '명시적(explicit) 동의'를 얻은 후에만 허용하도록 하고 있다. 이 '명시적 동의'에 대해서 네덜란드 데이터 보호 당국인 Autoriteit Persoonsgegevens의 가이드라인에서는 보다 명확하게 PSP가 제공하는 다른 서비스 이용약관과 별개로 개인 계좌정보 접근에 대한 동의를 받도록 하고, 형식은 온라인 팝업이나 체크방식 등을 취하도록 명시하고 있다[23].

우리나라 역시 이러한 추세를 따라 마이데이터 정책과 관련한 신용정보법 개정안에 동의서 양식 개정 내용을 반영하였다. 고지사항들을 단순화하고 쉽게 인지할 수 있도록 시각화하며, '동의등급제도'를 도입하여 정보주체가 자신의 동의에 따른 혜택과 사생활 침해 위험 등을 직관적으로 이해할 수 있도록 한다는

것이다[17].

금융위원회의 '동의등급제'안에 따르면 수집·이용·제공되는 정보의 내용에 대해서 정보주체에게 요약정보를 우선 제공하도록 하고, 고객이 요구할 경우 상세 정보도 함께 제공해야 한다. 또한 선택적 정보에 대해서는 정보 주체가 활용 목적별·기관별로 구분하여 개별적으로 동의여부를 선택할 수 있도록 하였고, 금융위원회는 정보 활용에 따른 프라이버시와 자유를 침해할 위험, 정보 주체가 얻는 이익이나 혜택 등을 종합적으로 평가하여 Table.4.와 같이 등급을 매긴 후, 해당 등급을 개인에게 알리고 동의를 받도록 하고 있다.

이러한 동의등급제는 기존의 지나치게 복잡하고 길었던 동의서 양식으로 인해 소비자들이 그 내용을 제대로 파악하지 못하고 형식적으로 동의한다는 문제를 개선하기 위한 것으로 그 취지와 방향은 타당한 것으로 판단된다. 하지만 현실적으로 금융위원회가 정보활용 동의 등급을 산정함에 있어 어려움이 예상된다, 다양하고 방대한 양의 각종 정보들의 활용 동의서들에 대해 적시에 등급을 산출해줄 수 있는 지, 또한 그 산출된 등급의 적정성이나 형평성은 어떻게 담보될 수 있는 지 등이 우려스럽다. 특히 맞춤형 서비스를 제공하는 마이데이터사업의 경우 다양한 정보의 수집과 활용이 전제되는 바, 동의등급 심사기준을 엄격하게 적용하여 일괄적으로 '매우 신중' 또는 '신중'으로 부여하게 되면, 소비자들은 이에 대한 동의를 거부할 확률이 크고, 결국 마이데이터 정책을 통해 이루고자 하였던 데이터 산업 활성화는 그만큼 멀어질 수 있다. 따라서 제도 운영과정에서 마이데이터 정책의 제약 요소가 되지 않으면서 정보주체의 권리를 강화하는 방향으로 합리적인 기준을 제시하는 것이 필요해 보인다.

Table 4. Consent Grading System

Division (%)	Definition
Sensitivity of Collected data and privacy risk (50%)	- Range and sensitivity of collected data or data provided to the third party Privacy issue and degree of damage when data breach occurs
Data utilization (40%)	- Retention period, purpose and benefits of data utilization
Consumer-friendliness (10%)	How easy to recognize and understand the consent form
Consent Grading System: 4 Levels (proper, relatively proper, discreet, very discreet)	

5.2 이용 및 제공 단계: 제공 방식의 보안성 확보

정보주체자의 주도 하에 개인의 금융정보 활용 및 유통과정에서 정보보호와 보안적 측면에서 안전성과 신뢰성이 보장하는 것은 마이데이터 정책의 기술적 제도의 핵심이라 할 수 있다. EU와 우리나라 정부에서는 이에 대한 대책으로 1)강력한 본인인증 절차와 2)금융회사와 핀테크 업체간의 안전하고 신뢰할 수 있는 정보 제공 방식으로 API 사용 의무화를 제시하고 있다.

5.2.1 강력한 본인인증 절차의 이행

첫 번째로 데이터 이용 및 제공 대상에 대한 강력한 본인 인증 절차의 의무화이다. 마이데이터 정책으로 인해 정보의 활용 범위와 영향이 광범위해진 만큼 정보를 제공하는 금융기관과 정보를 수집하는 핀테크 사업자 모두 정보주체의 실수나 의도치 않은 거래가 이루지지 않도록 강력한 인증절차의 이행이 요구된다. EU RTS의 강력한 인증 방식(Strong Customer Authentication)에서는 본인 인증방식으로 지식기반, 소유기반, 생체기반의 인증방법 중 독립된 2가지 이상의 인증방법을 사용해야 한다고 명시하고 있다. 마이데이터 서비스의 비대면 업무 특성상 금융회사의 모바일뱅킹 서비스 등에 적용하는 수준의 비대면 실명확인 기술이 적용될 필요가 있다.

5.2.2 API 방식 의무화

두 번째로 금융회사와 핀테크 업체간의 안전하고 신뢰할 수 있는 정보 제공 방식의 지정이다. EU를 비롯한 우리나라는 보안상의 이유로 정보 제공 방식으로 API 방식을 채택하고 있다.

EU RTS의 공통적이고 안전한 개방형 통신을 위한 기준(Common and secure open standards

of communication)에서는 고객의 중요 인증정보(credentials)를 저장·이용하여 고객계좌정보를 보유한 은행사이트에 대리 접속하여 필요한 정보를 얻어내는 'Screen scraping' 방식은 원칙적으로 금지하고 API를 통한 계좌정보 접근이 이루어지도록 하고 있다[20].

금융위원회 역시 현재 핀테크 회사가 많이 활용하고 있는 'Screen scraping' 방식을 금지하고, 표준API 방식을 사용하도록 하고 있다. 하지만, 마이데이터 사업자의 API 방식 사용의무에는 다음과 같이 선결되어야 할 사항들이 있다.

첫째로 금융기관의 API 제공 의무화이다. 그동안 핀테크업체 등의 제3자 서비스 회사 입장에서는 금융기관에 고객 정보에 대한 접근을 위한 인터페이스 제공을 강제화하는 제도가 없었기 때문에, 은행에 의존하지 않고 가장 손쉽게 고객의 금융정보를 얻을 수 있는 방법으로 'Screen Scraping'을 이용한 것이다. 현실적으로 API방식은 전송 데이터의 범위와 그에 대한 표준 등을 정하여 개발이 데이터를 제공하는 금융회사에서 먼저 이루어져야만 서비스가 가능하다. 이같은 부분이 제도적으로 강제화되지 않는다면 기존 금융회사 입장에서도 고객과의 접점을 잃을 수 있는 상황에서 제3자 회사에게 자신들의 고객 데이터 및 금융 플랫폼을 개방하기 위해 시간과 비용을 들여서 API를 개발하고 운영할 이유가 없어 보인다.

두 번째는 API 제공을 위한 비용과 부담주체에 대한 문제이다. 표준API 시스템의 구축, 운영, 안전한 데이터 전송을 위한 비용에 대해서도 실무적인 논의가 필요하다. 비용 부담 부분에 있어서는 EU PSD2에서는 은행 등의 ASPSP이 TPP에 고객 계좌정보에 대한 접근을 무료로 제공하도록 명시하고 있어 정보제공자인 은행이 100% 부담하는 방향으로 가고 있는 것에 반해, 우리나라는 정보수신자인 마이데이터 사업자에게 일정 수준의 비용을 부담하도록 하고 있다. 신용정보법 개정안에 따르면 본인신용정보관리업자에게 대통령령으로 정한 산정기준에 따른 비용을 부담시킬수 있다라고 명시되어 있다. 실제 비용이 얼마나 청구될지 모르겠지만, 적정한 수준의 서비스 수수료 산정이 마이데이터 정책 활성화에 중요한 요소가 될 것으로 보인다.

마지막으로 금융기관의 핀테크 업자 차별금지 조항 포함여부이다. EU의 PSD2에는 제3자 서비스업자가 기존 금융기관에 의해 차별 받아서는 안된다는 조항이 포함되어 있다. 즉 고객이 금융기관에서 직접 업무를 처리하는 것과 제3자가 고객을 대신하여 업무를 처리하는 것이 모두 동등하게 취급받아야 하며, 금융기관이 비용이나 처리순서, 업무시간 등에서 이들을 차별해서는 안된다는 것이다.

이러한 부분이 국내에서도 전자금융거래법 개정 등을 통해 반영되어 API 방식을 통한 안전한 데이터 전송을 활성화하여 궁극적으로 마이데이터 정책을 통해 목표한 금융 산업 경쟁력 제고가 이루어 질 수 있도록 하여야 하겠다.

5.3 저장 및 파기 단계: 정보처리자의 책임 및 의무 강화

5.3.1 예방 중심의 개인정보 보호원칙 설계

EU GDPR이 구체적인 기술적·조직적 조치를 상세하게 규정하지 않는 반면 국내의 경우 금융분야 개인정보처리 보안과 관련된 기술적·조직적 조치에 대해 신용정보법, 전자금융거래법, 전자금융감독규정 등에서 구체적으로 규정하고 있는 편이다. 즉 1) 내부관리계획 수립·시행 2) 접근권한의 관리 3) 접근통제 4)암호화 5) 접속기록의 보관 및 점검 6) 악성프로그램 등 방지 7) 물리적 안전조치 규정 8) 출력·복사시 보호조치 9) 개인정보의 이용 제한 등 10) 파기 등의 내용을 자세히 규정하고 있다. 다만, '컨트롤러가 어플리케이션, 서비스, 제품 등 개인정보 처리수단의 설계 및 디자인 단계부터 처리 당시 시점까지 정보주체를 보호하기 위한 기술적·조직적 보호조치를 염두에 두어야 한다'는 GDPR 제25조 설계 및 기본 설정을 통한 정보보호(Data Protection by Design and by Default) 규정에 대해서는 아직 국내 법령에는 이와 관련된 규정이 존재하지 않는다. 현재 EU회원국은 물론 미국, 캐나다, 일본, 싱가포르 등 해외 주요국은 법률이나 가이드라인을 통하여 '설계에 의한 개인정보보호 원칙'을 정하고 있는 실정이다[22]. 우리나라도 해당 원칙을 국내 법령에 도입하여 개인정보 처리를 위한 기술과 시스템 설계의 초기 단계부터 개인정보보호의 문제를 고려한다면 정보주체의 권익도 보호하면서 데이터를 활용할 수 있을 것으로 기대된다.

5.3.2 개인정보영향평가(PIA)의 의무화 및 평가공개

위의 '설계에 의한 개인정보보호 원칙'과 관련하여

마이데이터 정책 등으로 인해 대량의 개인정보를 다루는 개인정보처리자에 대해서 개인정보영향평가(PIA)의 의무화도 고려해볼 필요가 있다.

개인정보영향평가(Privacy Impact Assessment, PIA)는 개인정보를 취급·활용하는 정보시스템을 신규로 구축하거나 기존 정보시스템의 중대한 변경 시 개인정보에 미치는 영향을 사전에 조사·예측·검토하여 개선방안을 도출하는 체계적인 절차로 시스템의 구축·변경 등을 완료하기 전에 사전적 평가 수행을 통해 사업의 시행이 정보주체의 프라이버시에 미치는 중대한 영향을 사전에 파악하고 그 영향을 줄이거나 없앨 수 있는 방안을 모색하는 것이다. 현행 개인정보보호법 제33조와 시행령 제35조에서는 일정규모 이상의 개인정보 파일을 운영하는 공공기관의 경우 개인정보 영향평가를 의무적으로 수행하도록 하고 있지만, 민간기관에 대해서는 의무사항이 아니다.

GDPR의 경우, 데이터 처리 대상에 대한 높은 위험도(High Risk)를 초래하는 새로운 처리 활용이 제안된 경우나 정보주체의 평가, 자동화된 의사결정, 체계적인 모니터링이 수반되는 경우 민간기관 역시 의무 대상으로 하고 있다. 따라서 유럽의 경우 마이데이터 사업자는 대량의 금융 데이터를 다루기 때문에 시스템 설계나 시스템의 중대 변경시 사전에 개인정보영향평가(PIA)를 받아 그 결과를 공개하는 것이 의무사항이다.

국내에서도 대량의 금융정보를 다루는 마이데이터 사업자와 같은 민간 기업에 대해서 PIA 제도를 의무화하고 그 평가 결과를 공개하여 소비자의 권리를 보장하고 개인정보보호를 실현할 필요가 있다.

5.3.3 DPO 지정 의무화

마지막으로 DPO(Data protection officer)의 지정 의무화를 들 수 있다. DPO는 조직 내에서 데이터 보호 문제의 주요 접점을 제공하는 자로, GDPR 제37조에서는 1)공공기관 2)대규모의 체계적인 모니터링에 종사하는 조직 3)민감한 개인데이터의 대규모 처리에 종사하는 조직의 요건에 1개라도 해당되는 경우 개인정보처리자는 DPO를 의무적으로 채용하도록 하고 있다. 마이데이터 사업자의 경우 기업의 핵심활동이 대규모의 개인정보를 정기적이고 체계적으로 모니터링하는 처리활동을 포함하기 때문에 DPO 지정을 해야하는 요건을 충족한다. GDPR상의 DPO는 현행 개인정보보호법 제31조의 '개인정보책임자'와 유사한 개념이나, DPO의 지위 보장 및 면책 규정 등 DPO의 실질적 활동을 보장하는 부분이 없다. DPO에 대한 보다 체계적인 연구와 그에 따른 국내 현행법상의 개인정보책임자의 지위와 역할에 관한 장단점 비교를 통한 우리나라 법체계에 맞는 DPO제도를 마련하여 도입할 필요가 있다[13].

VI. 결 론

본 연구에서는 인공지능, 로봇, 사물인터넷 등의 4차 산업혁명 시대를 맞이하여 그 비중과 가치가 매우 큰 개인정보에 대한 보호 및 활용에 대한 정책적 대안으로 제시된 마이데이터 정책을 유럽과 한국의 금융관련 법제 및 환경을 중심으로 종합적으로 비교·분석해보았다. 특히 EU의 PSD2로 야기된 오픈뱅킹(Open Banking) 트렌드는 전세계 금융 산업 내 강력한 혁신 드라이브를 제공하고, 국민 개개인에게 맞춤형 금융서비스를 제공하는 플랫폼 형성 등에 도움을 줄 것으로 기대된다. 하지만, 이러한 디지털 금융 혁신의 가속화 속에서 개인의 프라이버시 침해와 개인정보 오남용 및 유출에 대한 우려가 커진 것도 사실이다. 이에 본 연구에서는 금융분야 마이데이터 정책의 개인정보 생명주기별 위험을 단계별로 분석하고 이에 대한 대응 방안으로 1) 정보주체의 권리 강화, 2) 실효성 있는 동의 제도의 도입, 3) 데이터 전송방식의 보안성 확보, 4) 민간 데이터 처리자들의 관리 책임 및 의무 강화 등을 도출해 보았다.

본 연구는 유럽과 한국의 금융분야 마이데이터 정책들에 대한 종합적인 비교·분석을 수행하고 이를 통해 국내 금융분야 마이데이터 정책의 개인정보보호 강화를 위한 법적·제도적 방안들을 도출하였다는 것에 그 의의가 있다. 하지만, 각 방안별로 세부적인 적용방안을 수립하지 못했다는 것에는 한계점이 있다. 향후 연구에서는 금융회사 및 핀테크 사업자에게 실질적으로 적용 가능한 적용방안을 수립하고 검증하는 연구가 필요해 보인다.

References

[1] European Commision, "Building a European Data Economy(COM(2017) 9 final)", OCT. 2017.

[2] European Data Protection Supervisor,

"Report of workshop on Privacy, Consumers, Competition and Big Data 2 June", EDPS, 11 July. 2014.
〔3〕 Jun-Young Kim, "Review the Regulation and the Improvement in the Big Data - Focus on the policy directions and legislation of the new government", Kyungpook National University IT&Law Institue, IT and law study 15, pp. 157-191, Aug. 2017.
〔4〕 Hye-Sun Yoon, "A Search for a New Regulatory Paradigm for Big Data - Is a shift into the risk-based regulation feasible?", Economic Regulation and Law, 11(1), pp.71-94, 2018.
〔5〕 Korea Data Agency, "2018 Data Industry White Paper", Korea Data Agency, 2018.
〔6〕 Joo-seok Park, "A Comparative Study of Big Data, Open Data, and My Data", The Korean journal of bigdata, pp. 41-46, 2018.
〔7〕 Financial Services Commission, "Data Protection and Utilization Measures in the Financial sector", Mar. 2018.
〔8〕 Financial Services Commission, "Introduction of Mydata Industry in the Financial Sector for Consumer-oriented financial innovation", July. 2018.
〔9〕 General Data Protection Regulation (EU) 2016/679.
〔10〕 Park, Whon-Il, "Is Data Portability Available in Korea?", The Institute of Legal Studies, Kyunghee University, pp. 211-232, 2017.
〔11〕 Gwon Min-Gyeong, "Current Status and Implications of Domestic and Foreign My Data", Capital Markets Research Institute, Feb. 2019.
〔12〕 OBWG, "The Open Banking Standard", The Third Meeting of Payments Strategy Forum", 2016.
〔13〕 Soo-Young Cho, "A Study on Privacy Protection in the EU's GDPR and Korea's Personal Information Protection Act", Kyungpook National University Law Journal 61, pp.117-148, April. 2018.
〔14〕 European Commission, "Payment Services(PDS2) - Directive(EU) 2015/2366", Dec. 2015.
〔15〕 François de Witte, "The new service providers introduced by PSD2', PA Perspectives on Nordic Financial Services, Jan. 2017
〔16〕 Kyu-Sun Choi and Ji-Young Lee, "EU PSD2's Impact on the financial sector", KFTC, Oct. 2018.
〔17〕 Financial Services Commission, "Payment Services Infrastructure Innovation Plan for Fintech and Financial platform development", Feb. 2019.
〔18〕 Deloitte, "Open banking privacy at the epicentre", June. 2018.
〔19〕 The Constitutional Court 2005. 5. 26. Sentence 99-hun-ma-513 decision
〔20〕 European Commision, "Regulatory technical standards (RTS) for strong customer authentication(SCA) and common and secure open standards of communication(CSC)-Regulation(EU) 2018/389", Dec. 2017.
〔21〕 Financial Services Commission, "Fintech Innovation Activation Plan", March. 2018.
〔22〕 Na-Ru Kim, "A Study on the Introduction and Application of Privacy by design", The Institute for Comparative Legal Studies, 29(4), pp. 8-14, 2017.
〔23〕 Angus McFadyen, ″Dutch data watchdog: PSD2 consent must be obtained ′separately′″, Outlaw.com, Nov. 2018.

〈저자소개〉

송 미 정 (Mi-Jung Song) 정회원
2003년 2월: 숙명여자대학교 컴퓨터과학과 졸업
2018년 3월~현재: 고려대학교 정보보호대학원 석사과정
2003년 1월~ 현재: 한국산업은행 근무
〈관심분야〉 전자금융보안, 금융 IT 컴플라이언스, 핀테크

김 인 석 (In-seok Kim) 종신회원
2008년: 고려대학교 정보경영공학과 (박사)
2009년~현재: 고려대학교 정보보호대학원 교수, FDS산업포럼 회장, 한국정보보호학회 운영위원
〈관심분야〉 전자금융보안, 금융 IT 컴플라이언스, 핀테크