금융분야 마이데이터 추진 현황

2019. 11. 29.

금융보안원
FINANCIAL SECURITY INSTITUTE

개인정보 관리·활용 패러다임 변화 (1)

"Personal data is the new oil of the Internet and the new currency of the digital world."

(Meglena Kuneva, European Customer Comminsioner, March 2009)

'personal will be the new oil – a valuable resource of the 21th century'

(Personal Data: The Emergence of a New Asset Class, World Economic Forum, 2011.2.)

- 광범위한 개인(신용) 정보(데이터)로 인한 사생활 침해, 개인정보유출 우려
- 자신의 개인(신용)정보를 통제·관리 불가능

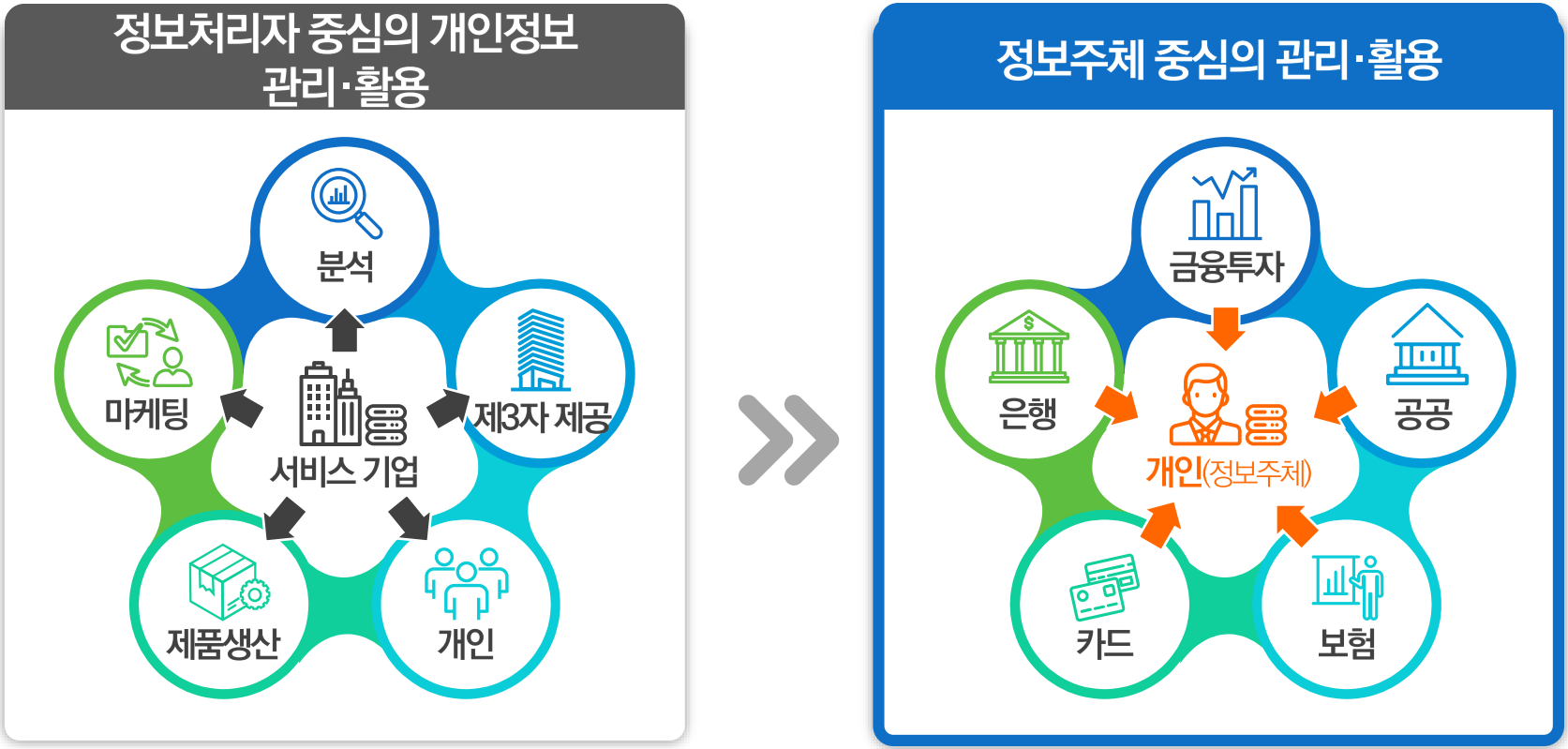
"디지털 시대에 경쟁과 혁신을 촉진, 소비자에게 더 나은 선택과 서비스를 제공"

"정보주체(개인)과 관련된 개인(신용)정보를 개인의 의사에 따라 활용"

개인데이터를 관리하고 활용하는 새로운 인프라 수준의 접근

개인정보 관리·활용 패러다임 변화 (2)

[개인정보 자기결정권, 데이터 이동권]



정보처리자(기업) 중심 → 정보주체(개인) 중심

(MyData, Personal Data Storage)

국내·외 동향 (1)

영국 Midata

- (2011) Midata 프로젝트 추진
- (2013) MIL(Midata Inovation Lab) 시작
- (2018) Open Banking Standards로 오픈뱅킹 도입

프랑스 MesInfos

- (2012) MesInfos 프로젝트 추진
- (2016.10.) 디지털공화국법* 제정
- (2017) 디지털공화국법 발효

* 공공 데이터의 자유로운 활용, 국민의 인터넷 접근권 보장 등 데이터 개방 조항을 포함

미국 Smart Disclosure

- (2010) 도드 프랭크법*(Dodd-Frank Act) 발표
- (2012) GreenButton Initiative 출범
- (2016.3.) BlueButton S4S** 프로젝트 연계

* 소비자가 개인 금융데이터를 사용할 권한을 보장하고 단체가 금융 정보를 전자적 형태로 가공하여 소비자에 제공할 것을 규정

** Sync for Sciences, 개인이 자발적으로 의료정보를 기부할 수 있는 기술 개발

핀란드 MyData

- (2014) MyData 백서 발간
- (2014) DHR(Digital Health Revolution) 프로젝트
- (2017) MyData 아키텍처 프레임워크 마련

국내·외 동향 (2)

싱가포르 OpenBanking

- (2015.6.) 스마트 금융센터 출범 : 핀테크 산업 발전 5대 정책으로 오픈뱅킹 플랫폼 발표
- (2016) 오픈뱅킹 지침 발표

호주 CDR

- (2018.5.) CDR(Customer Data Right) 정책 발표
- (2019.5.) 은행분야 CDR 시행
- (2022.1.(예정)) 전분야 CDR 시행

EU

- (2015.12.) PSD2(개정지급결제서비스지침) 공표
- (2018.1.) PSD2 시행
- (2018.5.) GDPR 시행('개인정보이동권')

우리나라

- (2016.8.) 금융권(은행, 증권) 공동 오픈API 오픈플랫폼 구축
- (2018.7.) 금융분야 마이데이터 산업 도입 방안 발표
- (2019.11.) 오픈뱅킹 시행

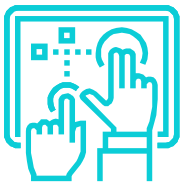
마이데이터 산업 도입

개인정보 자기결정권 보장

- 자기결정권 행사 기반 제공
- 전송요구권 도입
- 권리 대리 행사 지원

금융소비자 보호

- 정보 불균형 해소
- 맞춤형 정보·자문 서비스 제공
- 정보보호·우려 해소



금융산업 경쟁·혁신 촉진

- 금융社 정보독점 완화 및 경쟁 확산
- 혁신 산업·서비스 창출
- 고부가가치 산업 육성

개인신용정보 전송요구권을 보장하고
이를 기반으로 하는 마이데이터 산업을 도입

마이데이터 산업 도입 방향

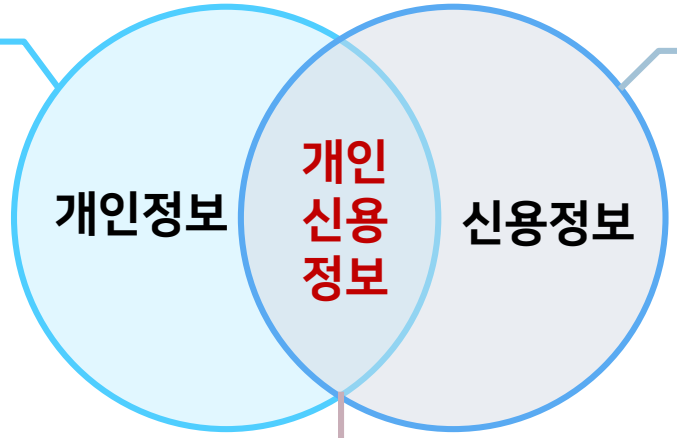
전송요구권 도입 및 안전한 마이데이터 생태계 조성을 위한 마이데이터 산업 규율체계 마련

개인신용정보

〈그 밖의 개인정보〉

신용도 판단과 무관한 정보로서 개인에 관한 정보

(임직원정보,영상정보, 거래상대방이 아닌 자의 정보, 상품소개 또는 구매권유 목적의 정보 등 신용정보법 미적용 고객정보 등)



〈그 밖의 신용정보〉

거래 상대방의 신용도 판단에 필요한 정보로서 기업 및 법인 정보 비식별 신용정보 등

(법인등록번호, 금융거래기록 등)

〈개인신용정보〉
거래 상대방의 신용도 판단에 필요한 정보로서 개인에 관한 정보

(연락처, 금융거래기록 등)

〈출처 : 금융분야 개인정보보호 가이드라인(2016.12)〉

개인신용정보 전송요구권 (1)

개인신용정보 전송요구권 도입

- 신용정보주체가 본인의 개인신용정보를 **본인, 본인신용정보관리회사 등을 포함하여 대통령령이 정하는 자**에게 **전송을 요구**할 수 있도록 보장
- 정보의 정확성·최신성을 위해 **정기적 전송 요구 가능**

제33조의2(개인신용정보의 전송요구) ① 개인인 신용정보주체는 대통령령으로 정하는 신용정보제공·이용자나 「개인정보 보호법」에 따른 공공기관으로서 대통령령으로 정하는 공공기관(이하 이 조 및 제33조의4에서 "신용정보제공·이용자등"이라 한다)에 대하여 그가 보유하고 있는 본인에 관한 개인신용정보를 다음 각 호의 어느 하나에 해당하는 자에게 전송하여 줄 것을 요구할 수 있다.

1. 해당 신용정보주체 본인
2. 본인신용정보관리회사
3. 대통령령으로 정하는 신용정보제공·이용자
4. 개인신용평가회사
5. 그 밖에 대통령령으로 정하는 자

개인신용정보 전송요구권 (2)

금융회사에 신용정보 제공 의무 부여

- 정보주체의 전송요청에 응하지 않을 경우 과태료 부과

제52조(과태료) ③ 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.
(중략)
6의2. 제33조의2제3항 또는 제4항을 위반하여 개인신용정보를 전송하지 아니한 자

전송요구 권리행사 위임

- 정보주체는 본인의 개인신용정보 전송요구를 대리인에게 위임 가능

제39조의3(신용정보주체의 권리행사 방법 및 절차) ① 신용정보주체는 다음 각 호의 권리행사(이하 “열람등요구”라 한다)를 서면 등 대통령령으로 정하는 방법 · 절차에 따라 대리인에게 하게 할 수 있다.
1. 제33조의2제1항에 따른 전송요구

본인신용정보관리업(마이데이터) (1)

본인신용정보관리업 신설 (마이데이터 산업)

- 정보주체의 개인신용정보 관리를 지원하는 본인신용정보관리업 신설

9의2. “본인신용정보관리업”이란 개인인 신용정보주체의 신용관리를 지원하기 위하여 다음 각 목의 전부 또는 일부의 신용정보를 대통령령으로 정하는 방식으로 통합하여 그 신용정보주체에게 제공하는 행위를 영업으로 하는 것을 말한다.

가. 제1호의3가목1) · 2) 및 나목의 신용정보로서 대통령령으로 정하는 정보 (여수신, 카드 거래내역)

나. 제1호의3다목의 신용정보로서 대통령령으로 정하는 정보 (보험)

다. 제1호의3라목의 신용정보로서 대통령령으로 정하는 정보 (금융투자)

라. 제1호의3마목의 신용정보로서 대통령령으로 정하는 정보 (상거래)

마. 그 밖에 신용정보주체 본인의 신용관리를 위하여 필요한 정보로서 대통령령으로 정하는 정보

본인신용정보관리업(마이데이터) (2)

본인신용정보관리회사 업무

고유 업무

- 본인 신용정보 통합조회 서비스 제공

※ 신용조회업(CB)은 개인의 신용상태를 평가하여 제3자(금융회사 등)에게 제공하는 업무로 규정

부수 업무

- 개인정보 자기결정권의 대리행사 업무(전송요구권, 동의철회, 연락중지 등)
- 데이터 분석·컨설팅 및 제3자 제공 업무
- 정보계좌(Personal data account) 업무

겸영 업무

- 자본시장법 상의 투자자문·일임업
- 금융소비자보호법(안) 상의 금융상품자문업

* 법적 규율체계 정비될 때까지 금융상품 추천·비교공시를 부수업무로 허용

본인신용정보관리업(마이데이터) (3)

본인신용정보관리업(마이데이터) 진입 규제

진입 규제

- 최소자본금 5억원, 배상책임보험 가입 의무화
- 신용정보관리보호인 필수 인력 요건
- 정보처리시설 및 기술적, 물리적 보안시설 구비

정보 보안

- (개인신용정보 이동권 행사 여부 확인을 위한) 강력한 본인인증

  * 본인여부가 확인되지 아니하는 등 대통령령으로 정한 경우에는 전송요구 거절 또는 전송 정지·중단

- API 방식으로 데이터 전송 (개정안 제22조의10)
- 개인신용정보 활용·관리실태 상시평가 대상 (개정안 45조의5)

정보주체의 접근매체 사용 제한 등

개인신용정보 수집·전송 기준

- 마이데이터 사업자가 **정보주체의 접근매체 등을 사용**하여 개인신용정보를 수집하는 것을 **제한**
- 정보주체 요청에 따라 금융회사 등이 마이데이터 사업자에 개인신용정 전송시에는 **안전성·신뢰성 보장이 가능한 방식으로 직접 전송**

※ 제14조 ②항에 따라 위반시 6개월 이내 업무정지 가능, 제52조 ②항에 따라 위반시 5천만원 이하 과태로 부과 가능

제22조의10(본인신용정보관리업에 따른 법률관계) ① 본인신용정보관리회사는 다음 각 호의 수단 또는 정보를 대통령령으로 정하는 방식으로 사용 · 보관함으로써 신용정보주체에게 제공할 신용정보를 수집하여서는 아니된다.

1. 제33조의2제1항에서 정하는 신용정보제공 · 이용자등이 선정하여 사용 · 관리하는 신용정보주체 본인에 관한 수단 · 정보로서 「전자금융거래법」 제2조제10호에 따른 접근매체

2. (중략)

② 제33조의2제1항에서 정하는 신용정보제공 · 이용자등은 (중략) 정보제공의 안전성과 신뢰성이 보장될 수 있는 방식으로서 대통령령으로 정하는 방식으로 해당 개인인 신용정보주체의 개인신용정보를 그 본인신용정보관리회사에 직접 전송하여야 한다.

개인신용정보 전송요구 대상 정보

전송요구 대상 정보 범위

- **제33조의2에 따라 신용정보주체가 전송을 요구할 수 있는 본인에 관한 개인신용정보의 범위는 대통령령으로 정함**

제33조의2(개인신용정보의 전송요구) ① (중략)

② 제1항에 따라 개인인 신용정보주체가 전송을 요구할 수 있는 본인에 관한 개인신용정보의 범위는 다음 각 호의 요소를 모두 고려하여 대통령령으로 정한다.

1. 해당 신용정보주체(법령 등에 따라 그 신용정보주체의 신용정보를 처리하는 자를 포함한다. 이하 이 호에서 같다)와 신용정보제공 · 이용자등 사이에서 처리된 신용정보로서 다음 각 목의 어느 하나에 해당하는 정보일 것

가. 신용정보제공 · 이용자등이 신용정보주체로부터 수집한 정보

나. 신용정보주체가 신용정보제공 · 이용자등에게 제공한 정보

다. 신용정보주체와 신용정보제공 · 이용자등 간의 권리 · 의무 관계에서 생성된 정보

2. 컴퓨터 등 정보처리장치로 처리된 신용정보일 것

3. 신용정보제공 · 이용자등이 개인신용정보를 기초로 별도로 생성하거나 가공한 신용정보가 아닐 것

개인신용정보 전송요구 대상 및 수수료

전송요구 대상 기관 범위

- 제33조의2에 따라 전송요구 대상 기관은 대통령령으로 정하며 **기본적으로 본인신용정보관리 회사도 포함**

  - 정보주체는 본인신용정보관리회사에 이동한 본인의 정보를 제3의 본인신용정보관리회사 또는 대통령령으로 정한 자에게 이동 가능

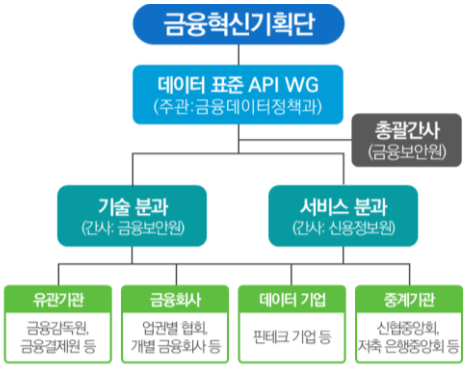
전송 수수료 기준

- 금융회사 등은 개인신용정보를 **정기적으로 전송할 경우**에는 **대통령령으로 정한 산정기준**에 따라 필요한 범위내 **최소한의 비용**은 마이데이터 사업자에 부과 가능

「데이터 표준 API」 워킹그룹

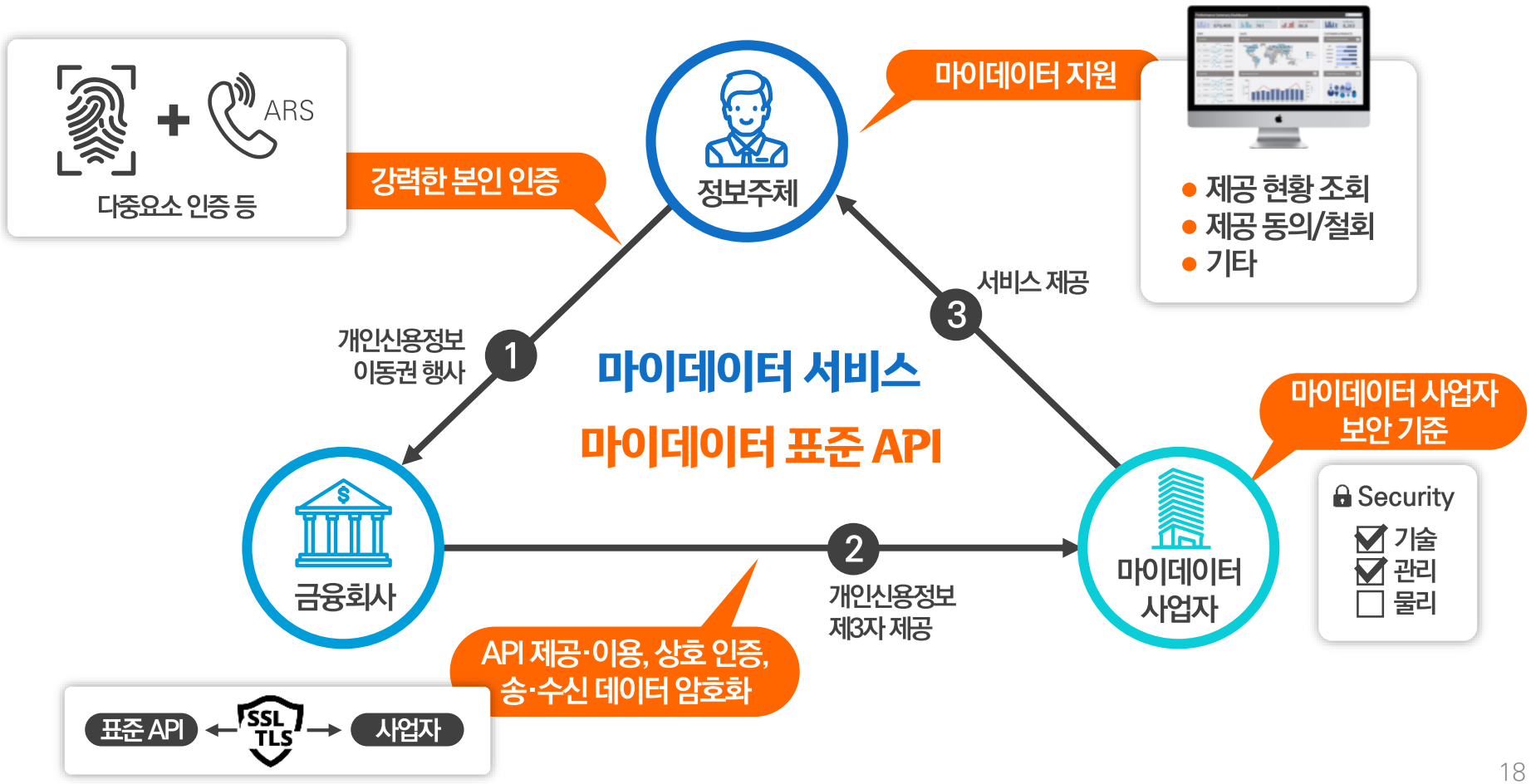
(목적) 신용정보법 개정에 따라 마이데이터 서비스가 신속·차질없이 운영될 수 있도록 API 규격 등 필요사항을 사전 준비

- (1차) '19.4.30. ~ 8.30 (4개월)
- (2차) '19. 11월 ~ '20. 4월 (6개월) 예정
  - ➢ 정부, 유관기관, 금융회사, 핀테크 기업 등 60여개 社 구성
- 이동 대상 데이터, 업무절차, 인증방법, API 규격, 보안 가이드라인 등 협의



금융분야 마이데이터 서비스

[마이데이터 기술(인증, API 등)의 표준화를 통해 보안성·안정성·확장성·편의성 제고]



주요 논의주제 (1/3)

1 개인신용정보 전송요구권(이동권) 관련

- **정보주체 및 정보제공자 범위**

  * (정보주체) 미성년자, 외국인 등, (정보제공자) 금융회사, 전자금융업자, 핀테크 기업 등

- **제공정보 범위 논의 (대상정보, 대상기간 등)**

  * 전자금융업자 및 핀테크 기업이 보유한 개인신용정보 대상 등

  * 호주, 영국 등 해외 사례 참고 , 정보제공 범위를 단계적으로 확대하는 방안 등

- **정보주체에 직접 전송요구 및 정기적 전송요구시 정보 제공 방법**

  * 정보주체에게 직접 제공 방법 (호주는 human-readable)

- **정보제공 항목(전송 데이터) 표준화 등**

주요 논의주제 (2/3)

2 마이데이터 서비스 기준 및 절차

- 마이데이터 서비스 참조 모델 및 절차 마련

  * 서비스 이용 접점별(서비스 앱 등) 표준 이용 참조 모델·절차 설계

- 개인신용정보 유출 등 사고 발생시 손해배상 기준 등

3 API 기술규격

- 데이터 전송 API 요청 및 응답 규격

  * REST API, JSON, JWT, OAuth 2.0 등의 기술규격 준용 검토

- 사용자 인증 절차·방식, API 접근권한 부여 세부규격 등

  - 개인신용정보 이동권 행사 여부에 대한 정보제공기관의 명확한 인증 필요

    * 핀테크 기업은 간편인증 선호, 고객 접점 확보 문제

  - 개별인증 / 통합인증 (WebView 방식 등)

주요 논의주제 (3/3)

4 마이데이터 서비스 지원 체계

- 정보주체의 본인정보 이동 현황 관리

  * 이동현황 통합조회, 전송요구 동의·변경·철회 정보 등 (정보주체의 실질적인 자기정보결정권 보장방안 등)

- 마이데이터 서비스 운영·보안 지원

  * 마이데이터 서비스 등록 정보, API 제공 정보, 위협정보, API 성능 통계 등

- 마이데이터 서비스, API 개발 및 테스트 지원 세부 방안(테스트베드 등)

5 운영·보안 가이드라인

- 법·규정 준수사항, 비정상 API 접근 모니터링 등

(참고) 호주 소비자 데이터 권리 규정

CDR 정책의 은행 분야 적용 원칙 및 기준

- Competition and Consumer(Consumer Data Right) Rules 2019 주요 내용

데이터 최소화 원칙 +

소비자에 관한 데이터 요청 시 합리적으로 필요한 수준보다 많거나 장기간의 데이터를 수집·사용하는 것을 제한

명확·간결한 동의 요구 +

소비자가 명확하고 쉽게 이해할 수 있도록 동의를 요구하도록 규정

※ 간결한 언어 및 시각적 보조자료 활용, 타 동의와 병행 금지 등

데이터 보호 대책 마련

정보보안 거버넌스 체계 수립, 정보보안 역량 확보, 평가 체계 수립, 사고 대응 및 보고 등 보안 대책 마련을 요구

게이트웨이 지정 제한 +

데이터를 중계하는 게이트웨이는 기 구축된 데이터 접근 채널이 부족한 경우에 한해 지정(은행분야는 미지정)

데이터 표준 준수

표준 전담 기관을 지정*하여, 데이터 및 인증 규격, 참여자 관리 규격, 서비스 UI 및 절차를 제공, 이를 준수토록 규정

* 사이버 보안, 개인정보 보호, 신기술 연구 등을 수행하는 연방연구소('Data 61')를 표준 전담 기관으로 지정

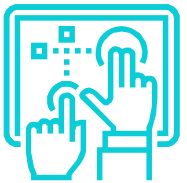
기대 효과

개인신용정보 자기결정권 보장

- 자기결정권 행사 기반 제공
- 전송요구권 도입
- 권리 대리 행사 지원

금융소비자 보호

- 정보 불균형 해소
- 맞춤형 정보·자문 서비스 제공
- 정보보호·우려 해소



금융산업 경쟁·혁신 촉진

- 금융社 정보독점 완화 및 경쟁 확산
- 혁신 산업·서비스 창출
- 고부가가치 산업 육성

감사합니다

금융보안원
FINANCIAL SECURITY INSTITUTE