6 Q&A

1. 개인신용정보 전송

궁금해요?

Q 기관간 개인신용정보 전송 요구 시 전송할 수 있는 데이터 범위는?

신용정보법 제33조의2②에 따르며 구체적인 내용은 신용정보원이 제공하는 금융분야 서비스 가이드라인 3.3.을 참고바랍니다.

A

Q 마이데이터사업자도 개인신용정보 전송요구에 응해야 하는지?

마이데이터사업자는 신용정보법 제33조의2에 따른 데이터정보제공·이용자등(정보제공자)에 포함되어, 동법 제33조의2②항에 해당하는 개인신용정보에 대해 고객의 개인신용정보 전송요구에 응하여야 합니다. 단, 타 정보제공자를 통해 수집한 정보는 전송의무를 가지고 있지 않습니다.

* 고객의 개인신용정보 전송요구에 응하여야 하는 기관 정보는 [참고1]정보제공자·정보수신자 범위 참고

A

Q 고객, 마이데이터사업자 외에도 개인신용정보를 전송받을 수 있는지?

고객, 마이데이터사업자 외에 신용정보법령에 따라 개인신용정보를 수신할 수 있는 금융기관은 고객의 개인신용정보전송 요구에 따라 개인신용정보를 수신할 수 있습니다.
* 고객의 개인신용정보 전송요구에 의해 개인신용정보를 수신가능한 기관 정보는 [참고1]정보제공자·정보수신자 범위 참고

A

Q 마이데이터사업자에게 API를 이용하여 개인신용정보를 전송할 경우, 중계기관을 이용하여 전송할 수 있는지?

신용정보업 감독규정(제23조의3③)에 정의된 기관 외의 기관은 중계기관을 이용하여 개인신용정보 전송 수행이 가능합니다. 다만 그 외의 기관은 자체적으로 시스템를 구축하여 개인신용정보를 전송하여야 합니다.

A

Q 개인신용정보 전송 요구 시 비밀계좌, 보안계좌 등이 표기되지 않는데, 고객은 이를 전송 요구할 수 없는지?

비밀계좌, 보안계좌 등과 같이 고객이 비대면 정보 조회 금지를 요청한 정보를 원칙적으로 개인신용정보 전송요구 대상에서 제외되어 전송요구시 표기되지 않습니다. 이 경우 고객이 금융회사 창구등을 통해 해당 정보에 대하여 일반계좌로 전환 시 개인신용정보 전송요구가 가능합니다.

A

Q 중계기관을 이용하여 개인신용정보를 전송할 경우 해당 개인신용정보는 중계기관에서 저장·보관하는지?

A 중계기관은 개인신용정보 전송을 중계할 뿐 해당 개인신용정보를 별도로 저장·보관할 수 없습니다.

Q 마이데이터사업자는 정보제공자에 정기적 전송을 요구할 수 있는데, 주기에 따른 전송 횟수 제한이 있는지?

A 개인신용정보의 정확성 및 최신성 유지를 위해 마이데이터사업자는 최대 1주 1회*에 한하여 동일한 내역의 개인신용정보를 정보제공자에 전송 요청 가능합니다. 단, 고객이 직접 개입한 경우(조회, 새로고침 등)는 횟수 제한 없이 전송 요청이 가능합니다.
*1주의 기준은 일요일에서 토요일로 함

Q 정기적 전송 중 개인신용정보 전송 지연이 발생하였을 때도 고객에게 지연고지를 하여야 하는지?

A 정기적 전송이 고객의 명시적인 요구 행위가 아닌점, 또한 정기적 전송이 통상 야간, 새벽등에 발생하여 지연고지 시 고객 불편이 발생할 수 있는 점 등을 고려하여 정기적 전송에 한해 고객에 지연고지 의무가 면제됩니다.

Q 지체없이 전송에서 지체없이의 의미는?

고객이 정보 전송을 요구하는 시점에서 정보제공자가 시스템의 처리시간에 따라 정보를 즉시 전송하는 것을 의미합니다.

A

Q 개인신용정보 전송요구시 별도의 동의절차가 있는지?

신용정보법령에서 요구하는 동의절차외에 별도로 지원기관이 정의하는 '알고하는 동의절차'를 적용해야 합니다.

A

2. 마이데이터서비스

궁금해요?

Q 마이데이터사업자 허가를 위한 절차는?

A 신용정보업 감독규정 별표1(본인신용정보관리업 허가 등의 절차) 또는 본 가이드라인의 [참고2] 참고바랍니다.

Q 마이데이터서비스는 모바일 앱만을 의미하며 브라우저를 통한 웹서비스는 해당되지 않는지?

A 기능확장, 정보보호·보안 등을 고려하여 현재는 모바일 앱서비스를 고려하여 가이드라인이 구성되어 있습니다. 다만, 통합조회등의 마이데이터서비스는 웹을 이용하여서도 제공이 가능합니다.

Q 가이드라인 내 용어를 필수적으로 이용하여야 하나요?

A 고객 편의성을 위하여 고객에게 익숙한 용어로 변경하여 이용가능합니다. (예, 개인신용정보 전송 철회 → 연동 해제 등)

Q 전용앱이 아닌 뱅킹 앱 등 별도서비스의 인앱(in-app)형태로 마이데이터 서비스를 제공할 경우도 별도의 마이데이터 서비스 회원가입/탈퇴 절차가 필요한가요?

A 전용앱이 아닌 인앱 형태로 마이데이터 서비스를 제공하는 경우에도 고객의 마이데이터 서비스 회원가입(또는 별도의 서비스 이용 동의)을 받아야하며, 마이데이터 서비스 회원탈퇴(또는 별도의 서비스 이용 해지) 기능을 제공하여야 합니다.

Q 마이데이터사업자의 영업 범위는 본인신용정보 통합조회 서비스로 한정되는지?

A 마이데이터사업자는 고유업무인 본인 신용정보통합조회 서비스 이외에 부수·겸영업무*에 속한 서비스 제공도 가능합니다.

* 부수업무: 수집한 개인신용정보를 기초로하는 데이터 분석 및 컨설팅 업무
* 겸영업무: 투자자문업 또는 투자일임업 등

Q 고객이 "전송을 요구하는 목적"을 특정할 시, 해당 내용을 고객이 직접문자열로 입력하는 형태가 아닌, 시스템에 기입력된 내용을 고객이 선택하는 방식으로 제공이 가능한지?

A 전송을 요구하는 목적 등 전송 시 특정사항은 신용정보원의 알고하는 동의 절차 및 기준을 준수하면 됩니다.

Q 통합인증을 통해 고객의 정보제공자 가입정보를 가져오고자 할 때, 한번에 선택할 수 있는 정보제공자 수가 제한되는지?

A 마이데이터 사업자는 고객편의, 전송요구 처리 부하등을 고려하여 최대 50개의 정보제공자를 고객이 한번에 선택할수 있도록 화면을 제공할 수 있습니다. 단, 고객은 마이데이터 사업자가 자율 구성한 정보제공자에 대해 개별적으로 추가·수정 선택할 수 있어야하며, 고객이 각 정보제공자를 개별적으로 추가 선택한 경우에는 50개 초과가 가능합니다.

Q 고객에게 두가지 인증수단(개별인증, 통합인증)을 모두 제공하여야 하나요?

A 마이데이터사업자는 통합인증을 반드시 제공하여야 하나, 개별인증은 제공여부를 선택가능합니다.

Q 기능적합성 심사 및 보안 취약점 정보에 대한 정보는 어디서 확인 가능한가요?

A 금융분야 마이데이터 테스트베드 내 자료실에서 확인 가능합니다.
*https://developers.mydatakorea.org

Q 웹, 모바일 등을 통해 수집한 개인신용정보를 이용하여 고객에게 대면 방식(금융창구 등)을 통한 마이데이터서비스 제공이 가능한지?

A 개인신용정보를 웹, 모바일 등을 통해 수집하였다 하더라도, 불완전 판매의 가능성이 있어 고객에게 대면 방식의 마이데이터서비스 제공은 할 수 없습니다.

Q 시행령 제18조의6제10항에 따라 연 1회 개인신용정보 전송 요구 내역을 탈퇴 고객에게도 통지하여야 하는지, 통지한다면 고객에게 통지하기 위해 탈퇴한 고객의 신용정보 전송요구내역에 관한 기록을 보관 가능한지?

A 1년 내 탈퇴한 고객에게도 통지하여야 합니다. 다만, 탈퇴 전 통지를 하였고 연 1회 통지 요건을 충족시킨 경우 통지하지 않아도 됩니다. 또한, 마이데이터사업자가 시행령 제18조의6제10항에 대한 통지 의무 이행을 위하여 기록을 보관하는 것은 법령상 의무 이행을 위하여 보관하는 것이므로 탈퇴 고객의 정보임에도 통지 시까지 신용정보 전송 내역 기록을 보관할 수 있습니다. (단, 수집한 개인신용정보는 탈퇴시 모두 삭제하여야함)

※ 서비스 가이드라인 Q&A의 Q20, Q21 참조(122p)

3. API

궁금해요?

Q 정보제공자가 고객에게 직접 개인신용정보를 전송할 때에도 API를 이용하여야 하는지?

A 고객이 요구한 개인신용정보를 정보제공자가 직접 전송할 시에는 PDS방식 등 별도로 정하는 바에 따릅니다.

Q 일시적인 API 요구 증가 등 망부하로 인해 전송요구에 응대가 어려울 경우 문제가 되는지?

A 일시적인 API 요구 증가로 인한 망부하로 인해 전송이 지연될 경우, 고객 에게 지연 사유를 통지하고 지연사유가 해소된 즉시 전송을 재개할 수 있습니다.

Q API전송구간은 전용망을 사용해야하는지?

A 규격에 따라 안전한 방식의 TLS를 활용할 경우 전용망이 필수는 아닙니다. 다만 더욱 안전한 전송을 위해 전용망 이용은 자율적으로 결정 할수 있습니다.

Q 정보제공자의 API시스템 구축 및 운영업무를 위수탁할 수 있는지?

금융기관 업무위탁 규정에 따라 정보제공자는 본질적 업무가 아닌 경우 외부업체와 위수탁계약을 맺어 업무수행이 가능합니다. 다만, 수탁사가 중계기관과 같이 다수의 정보제공자와 위수탁관계를 맺어 동일한 인터페이스로 다수의 마이데이터서비스 제공자에게 개인신용정보를 전송하는 형태는 불가합니다. (수탁 시스템이 계약을 맺는 위탁자만을 위한 전용시스템인 경우에 한해 가능)

A

Q 정보제공자는 접근토큰관리(발급, 인증 등)를 직접 수행하여야 하는지?

정보제공자등은 접근토큰 발급·인증 등 전반적인 접근토큰 관리는 직접 수행합니다. 발급된 접근토큰 내역은 종합포털에 전송되어 고객의 개인신용정보 전송요구 내역에 대한 통합 관리 지원에 이용됩니다.

A

Q 자격증명과 접근토큰의 차이가 무엇인지?

자격증명은 API 호출 시에 정보제공자와 마이데이터사업자간의 API 호출 자격을 인증하고 서로를 식별할 수 있도록 하는 것으로 종합포털이 정보제공자와 마이데이터 사업자에게 발급합니다. 반면 접근토큰은 마이데이터사업자가 개인신용정보 전송 요청 권한을 획득하기 위한 것으로 정보제공자가 마이데이터사업자에게 발급합니다. 접근토큰은 최대 유효기간이 1년이며 개인신용정보 전송 요구 변경·연장 시에 기발급된 접근 토큰을 폐기하고 재발급받아야 합니다.

A

Q API로 개인신용정보를 조회하는 경우 조회기간에 제한이 있는지?

정보수신자가 API방식을 통해 개인신용정보를 조회하는 경우 과도한 전송트래픽 집중, 정보제공자 API서버 과부하, 전송지연 등을 방지하기 위해 일(Date) 기준 API는 최대 31일, 월(Month) 기준 API는 최대 3개월로 조회기간(From/To)을 설정하여 요청하여야 합니다.

A

Q API규격에 따른 개발을 지원할수 있는 시스템이 있는지?

금융분야 마이데이터 테스트베드를 통해 테스트, 검증 등을 수행할 수 있습니다.
*https://developers.mydatakorea.org

A

Q 테스트베드에 대한 이용절차, 매뉴얼등이 있는지?

금융분야 마이데이터 테스트베드를 통해 확인 가능합니다.
*https://developers.mydatakorea.org

A

Q 토큰이 중복발급되었을 때 그 처리 절차는?

토큰이 중복발급되었을 경우, 해당 사실을 사업자에 통보하고 토큰 삭제 및 오전송 개인신용정보 유무 여부 확인 등 금융보안원이 정하는 후속 절차를 따라야 합니다.

A

4. 본인인증

궁금해요?

Q 정보제공자는 자사가 관리하는 특정한 인증수단 만을 제공해도 되는지?

A 정보제공자는 통합인증을 반드시 제공하여야 하며 개별인증 제공 여부는 선택가능합니다.

Q 정보제공자는 개별인증수단을 별도로 개발하여야 하는지?

A 정보제공자는 별도 자체 개발 또는 타 인증기관이 제공하는 인증방법(예:기존계좌활용 인증(1원 이체 등), 휴대폰 본인확인 등)을 이용하여 고객에 개별인증수단을 제공할 수 있습니다.

Q 중계기관을 이용하여 개인신용정보를 전송할 경우 본인인증 주체는?

A 정보제공자가 중계기관을 이용하여 개인신용정보를 전송할 경우, 중계기관이 정보제공자의 업무(본인인증)를 위탁하여 수행합니다. 이때, 고객이 통합인증을 이용하여 본인인증을 수행할 경우는 중계기관이, 개별인증을 이용하여 본인인증을 수행할 경우는 정보제공자가 본인인증을 수행하여야 합니다.

Q 정보제공자 또는 마이데이터사업자도 통합인증 수단 제공기관이 될 수 있는지?

A 통합인증을 위해서는 공통된 개인식별자(CI) 활용이 필요하며 CI활용에 문제가 없는 인증사업자는 가능합니다. 현재로서는('21년 2월) 적법하게 CI 제공이 가능한 정통망법상 본인확인기관과 전자서명법상 전자서명인증사업자(평가·인정 완료)등이 통합인증기관으로 참여 가능하며, 추후 개별법에 따라 CI활용이 가능한 경우 참여자격이 부여될 수 있습니다.

Q 개별인증 수단으로 휴대폰/신용카드 본인확인서비스 한가지만 적용 가능한지?

A SMS 인증 방식의 휴대폰 본인확인서비스는 다중요소 인증기준을 충족한다고 보기 어려우므로 추가적으로 지식 또는 특징 기반의 인증수단 적용이 필요합니다. 그 외 휴대폰 본인확인서비스 방식 및 신용카드 본인확인서비스 방식의 경우에는 다중요소 인증기준의 충족 여부와 안전성 등을 자율적으로 검토하시어 적용여부를 판단하시기 바랍니다.

Q 개별인증 수단으로 공동인증서, 또는 사설인증서 한가지만 적용 가능한지?

A 개별인증 수단으로는 다중인증, 다중요소 공개키인증서, 비대면실명확인 방식 활용 등을 적용 가능합니다. 공동인증서 및 일반적인 사설인증서는 다중요소 공개키인증서에 해당하므로 다른 인증수단 없이도 적용 가능합니다. 다만, 각 인증서 발급기관에 대한 신뢰성 및 안전성을 충분히 검토하시어 선정 및 적용하시기 바랍니다.

Q 개별인증 수단으로 사설인증서 적용시 반드시 전자서명법상 인정받은 전자서명인증사업자만 선정 및 적용하여야 하는지?

A 통합인증시에는 CI 제공·활용을 위해 사설인증기관의 경우에는 전자서명법상 인정받은 전자서명인증사업자 지위가 필요하지만, 개별인증시에는 CI 제공·활용이 필수가 아니기 때문에 필수 요건이 아닙니다. 다만, 전자서명법상 전자서명인증사업자의 평가·인정 여부는 사설인증기관 선정시 신뢰성 및 안전성 검토에 활용 가능합니다.

Q 통합인증에 따른 전자서명을 정보제공자 및 마이데이터 사업자가 저장·관리하여야 하는지?

A 전송요구내역의 보관 기준에 따라 저장·관리하여야 합니다.

Q 통합인증을 위한 사설인증서 적용시 별도 기준이 존재하는지?

A 마이데이터사업자는 공동인증서 외에 통합인증수단으로 포함된 사설인증서를 1개 이상 적용하여야 하며, 정보제공자는 통합인증처리를 위해 모든 통합인증수단(공동 및 사설인증서)을 허용하여야 합니다.

Q 고객이 기존에 발급받은 개별인증수단을 이용하는 중에 통합인증수단으로 본인인증 방식을 바꾼 후, 기발급된 개별인증수단도 계속 이용할 수 있는지?

A 개별인증수단은 각 정보제공자가 발급하는 인증수단으로 계속하여 이용 가능합니다.

5. 정보보호시설·보안

궁금해요?

Q 마이데이터사업자가 해외에 있는 상용클라우드를 이용할 수 있는지?

A 클라우드 사업자 안정성 평가 등 전자금융감독규정의 요건(제14조)을 지키는 경우에 한하여 이용이 가능합니다. (단, 개인신용정보는 국내에서 저장되어야 함)

Q 마이데이터사업자가 해외에 위치한 전산센터(IDC)를 이용할 수 있는지?

A 마이데이터사업자는 국내에 위치한 전산센터만 이용 가능합니다.

Q 망분리의 범위는 어디까지인지?

A 개인신용정보를 처리하는 서버, 서버에 접속하는 주요단말, 개인신용정보 관련 업무를 담당하는 담당자의 PC가 망분리 요건에 해당합니다.

Q 물리적 망분리 외에 논리적 망분리도 허용하는지?

서버와 서버에 접속하는 주요단말은 물리적 망분리, 업무PC는 물리적, 논리적 망분리를 적용하여야 합니다.

A

Q 정보제공자와 마이데이터사업자는 보안수준진단을 받도록 되어 있는데 구체적으로 어떠한 형태의 진단인지?

정보제공자와 마이데이터 사업자는 개정 신용정보법상 의무적으로 받아야하는 상시평가를 수행하면 보안수준진단을 수행하는 것으로 인정합니다.

A

Q 보안수준 진단을 위한 금융권 정보보호 상시평가는 평가를 담당하는 지정기관이 있는 것인지?

신용정보 감독규정 제45조의2에 따라 상시평가 점검 대상은 금융보안원에 점검 결과를 제출하여야 합니다.

A

Q 개보법상 개인정보보호책임자가 신정법상 신용정보관리·보호인을 겸임할 수 있는지?

개보법상 개인정보보호책임자가 신정법상 신용정보관리·보호인을 겸임하여 역할을 수행할 수 있습니다.

A

Q 마이데이터사업자는 주민등록번호를 처리할 수 있는지?

개정 신용정보법 시행령에 따라 주민등록번호 처리가 가능합니다. (신용정보법 시행령 제37조의2⑤항 참고)

A

Q 가입자 100만 이상의 마이데이터사업자가 금융보안원의 보안관제 서비스를 받기 위한 절차는?

금융보안원 사원가입을 통해 보안관제 서비스를 받을 수 있습니다.
※ 문의:02-3495-9122

A

Q 마이데이터 업무에 필요한 전산설비는 기존 업무에 필요한 전산설비와 구분하여 별도로 구축하여 운영해야 하는지?

정보보호에 미치는 영향을 자체검토하여 사업자 자율로 운영이 가능합니다.

A

Q 마이데이터서비스에 대한 보안취약점 점검 방법, 절차는?

마이데이터서비스는 서비스제공 이전 시점에서 보안취약점 점검을 받아야합니다.
(마이데이터 테스트베드 자료실 내 보안취약점 점검 안내서 참고)

A

Q 정보제공자간 API 호출 시 반드시 전용선(또는 VPN)을 의무사용해야하는지?

TLS를 안전하게 사용하는 경우(P.82 참조)에 한하여 전용선이 아닌 TLS를 사용가능합니다, 단, 정보제공자가 금융회사인 경우 중계기관과의 연결시 반드시 전용선 및 이에 준하는 연결을 하여야 합니다.

A

Q 안전한 TLS이용을 위해 특별히 요구되는 버전이 있는지?

안전한 TLS이용을 위해 TLS1.3을 이용하여야 합니다. 내부 여건으로 1.2를 이용하는 경우에는 가급적 신속하게 업데이트 하여야 합니다.

A