5 마이데이터 보안

본 장은 마이데이터서비스 제공과 관련하여 안전한 개인신용정보 전송, 저장 등의 처리를 위해 신용정보법령등에서 요구하는 보안요구사항등을 설명한다.

5.1. 마이데이터 보안 개요

가. 목 적

- 고객의 개인신용정보를 보유수집하는 정보제공자, 정보수신자는 안전한 개인신용정보 보호를 위해 본 가이드라인의 보안 준수사항을 참고하여 관리·운영 등에 적용하여야 한다.

나. 관련법규 및 규정

- 정보제공자 및 정보수신자는 개인신용정보 전송 및 마이데이터서비스 제공에 있어 신용정보법령 및 신용정보업 감독규정의 정보보호 조항을 준수하여야 한다.

관련법령

- **신용정보법 제19조(신용정보전산시스템의 안전보호)** ① 신용정보회사등은 신용정보전산시스템(제25조제6항에 따른 신용정보공동전산망을 포함한다. 이하 같다)에 대한 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험에 대하여 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을 수립·시행하여야 한다.

- **신용정보법 시행령 제6조(허가의 세부요건 등)** ① 법 제6조제1항 및 제3항에 따라 신용정보업, 본인신용정보관리업 또는 채권추심업의 허가를 받으려는 자가 갖추어야 할 인력 및 물적 시설의 세부요건은 다음 각 호의 구분에 따른다.

  1.~4. (생략)

  5. 본인신용정보관리업을 하는 경우: 제2항제2호에 따른 설비를 갖출 것

  ② 제1항 각 호(제4호는 제외한다)에 따른 상시고용인력 및 설비는 다음 각 호의 구분에 따른다.

  1. (생략)

  2. 설비: 신용정보 등의 처리를 적정하게 수행할 수 있다고 금융위원회가 정하여 고시하는 정보처리·정보통신 설비

- **신용정보업 감독규정 제6조(정보처리·정보통신설비)** 영 제6조제2항제2호에서 "금융위원회가 정하여 고시하는 정보처리·정보통신 설비"란 해당 신용정보업, 본인신용정보관리업 또는 채권추심업의 범위와 규모에 비추어 신용정보를 원활히 처리할 수 있는 수준의 정보처리·정보통신 설비로서 별표 2에 규정된 사항을 말한다.

- 마이데이터사업자 허가 시 망분리 기준 및 클라우드컴퓨팅서비스 이용등은 전자금융감독규정을 따른다.

관련법령

- **전자금융감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등)** ① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.

  1. 자체적으로 수립한 기준에 따른 이용대상 정보처리시스템의 중요도 평가

  2. 〈별표 2의2〉의 항목을 포함한 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등 평가

  3. 〈별표 2의3〉에서 정하는 사항을 반영한 자체 업무 위수탁 운영기준의 마련 및 준수

  ② 금융회사 또는 전자금융업자는 제1항에 따른 평가결과 및 자체 업무 위수탁 운영기준에 대하여 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

  ③~⑦ (생략)

⑧ 제2항의 절차를 거친 클라우드컴퓨팅서비스 제공자의 정보처리시스템이 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다. 다만, 금융회사 또는 전자금융업자(전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제대행업자는 제외한다)가 제3항제1호에 따른 고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.

⑨ (생략)

- **전자금융감독규정 제15조(해킹 등 방지대책)** ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

1.~2. (생략)

3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)

4. (생략)

5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.) 〈신설 2013. 12. 3., 개정 2015. 2. 3.〉

②~ ⑥ (생략)

- 개인신용정보의 보호는 특별법인 신용정보법을 우선 적용하고 신용정보법에 규정되지 않은 사항은 일반법인 개인정보보호법을 적용하여야 한다.

※ 개인신용정보를 제외한 개인정보는 개인정보보호법을 적용한다.

5.2. 관리적 보안사항

가 . 신용정보관리·보호인

○ **(신용정보관리·보호인 지정)** 정보제공자와 정보수신자는 개인신용정보 보호 계획 수립·시행 등의 업무 수행을 위해 신용정보의 관리·보호 등을 총괄하는 지위에 있는 사람을 신용정보관리·보호인*으로 지정하여야 한다.

* 개인정보보호법상 개인정보보호 책임자 겸임 가능

관련법령

- **신용정보법 제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존)** ③ 신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 제4항에 따른 업무를 하는 신용정보관리·보호인을 1명 이상 지정하여야 한다. 다만, 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 자는 신용정보관리·보호인을 임원(신용정보의 관리·보호 등을 총괄하는 지위에 있는 사람으로서 대통령령으로 정하는 사람을 포함한다)으로 하여야 한다.

신용정보관리·보호인의 자격

1. 사내이사
2. 집행임원(「상법」 제408조의2에 따라 집행임원을 둔 경우로 한정)
3. 신용정보의 제공·활용·보호 및 관리 등에 관한 업무집행 권한이 있는 사람(「상법」 제401조의2 제1항제3호에 해당하는 자)
4. 그 밖에 신용정보의 제공·활용·보호 및 관리 등을 총괄하는 위치에 있는 직원

– **(마이데이터사업자의 신용정보관리·보호인)** 마이데이터사업자는 신용정보관리·보호인을 임원 또는 집행임원, 신용정보의 제공·활용·보호 및 관리 등에 관한 업무 집행 권한이 있는 사람으로 지정하여야 한다.

- **(신용정보관리·보호인의 주업무)** 신용정보관리·보호인은 개인신용정보 보호 계획 수립·시행 등의 업무를 수행한다.

신용정보관리·보호인의 주업무

1. 개인신용정보 보호 계획의 수립 및 시행
2. 개인신용정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인신용정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인신용정보 누설 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인신용정보 보호 교육 계획의 수립 및 시행
6. 임직원 및 전속 모집인 등의 신용정보보호 관련 법령 및 규정 준수 여부 점검

- **(개인신용정보 관리 및 보호 실태 점검)** 신용정보관리·보호인은 신용정보관리·보호인의 주업무에 대하여 점검을 실시하고 보고하여야 한다.

개인신용정보 관리 및 보호 실태 점검

- **(점검 내용)**
  ① 신용정보관리·보호인의 주업무를 수행한 실적
  ② ①의 실적을 기재한 보고서를 대표이사 및 이사회에 보고한 실적
- **(점검 주기)** 연 1회 이상
- **(제출기한)** 매 사업연도 종료 후 3개월 이내
- **(제출처)** 금융위원회

☞ 신용정보관리·보호인 지정은 개인정보보호법상 개인정보보호 책임자와 겸임이 가능하며, 개인신용정보 보호 교육은 개인정보보호법상 개인정보보호 교육으로 갈음할 수 있다.

나. 개인신용정보 보호 교육

○ **(개인신용정보보호 교육)** 신용정보관리·보호인은 개인신용정보의 적정한 취급을 위하여 개인신용정보 보호 교육을 계획하고 수립하여 개인신용정보취급자에게 정기적인 교육*을 실시하여야 한다.

* 개인정보보호법상 개인정보보호 교육으로 갈음할 수 있다.

관련법령

- **신용정보법 제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존)** ④ 제3항에 따른 신용정보관리·보호인은 다음 각 호의 업무를 수행한다.

  2. 기업신용정보의 경우 다음 각 목의 업무

     마. 임직원 및 전속 모집인 등에 대한 신용정보보호 교육계획의 수립 및 시행

– **(개인신용정보보호 교육 계획 수립)** 교육 계획에는 교육 목적, 대상, 내용(프로그램 등 포함), 일정 및 방법 등을 포함하여 내부 관리계획 등에 규정하거나 별도의 교육 계획으로 수립한다.

– **(개인신용정보보호 교육 시행)** 조직 여건 및 환경에 따라 사내교육, 외부교육, 위탁교육, 온라인교육 등 다양한 방법으로 개인신용정보 보호 교육을 시행할 수 있다.

예시 **개인신용정보 보호 교육 예시**

- 개인신용정보 보호의 중요성
- 내부 관리계획의 제·개정에 따른 준수 및 이행
- 위험 및 대책이 포함된 조직 보안 정책, 보안지침, 지시 사항, 위험관리 전략
- 개인신용정보처리시스템의 안전한 운영·사용법(하드웨어, 소프트웨어 등)

- 개인신용정보 안전성 확보조치 기준
- 개인신용정보 보호업무의 절차, 책임, 방법
- 개인신용정보 처리 절차별 준수사항 및 금지사항
- 개인신용정보 누설·노출 및 침해신고 등에 따른 사실 확인 및 보고, 피해구제 절차 등

다. 개인신용정보 관리

○ **(신용정보 활용체제 공시)** 정보제공자는 신용정보활용체제를 작성하고 고객에게 공시하여야 한다.

관련법령

- **신용정보법 제31조(신용정보활용체제의 공시)** ① 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 다음 각 호의 사항을 대통령령으로 정하는 바에 따라 공시하여야 한다.

신용정보 활용체제 포함 사항

- 개인신용정보 보호 및 관리에 관한 기본계획(총자산, 종업원 수 등을 고려하여 대통령령으로 정하는 자로 한정한다)
- 관리하는 신용정보의 종류 및 이용 목적
- 신용정보를 제3자에게 제공하는 경우 제공하는 신용정보의 종류, 제공 대상, 제공받는 자의 이용 목적
- 신용정보의 보유 기간 및 이용 기간이 있는 경우 해당 기간, 신용정보 파기의 절차 및 방법
- 신용정보의 처리를 위탁하는 경우 그 업무의 내용 및 수탁자
- 신용정보주체의 권리와 그 행사 방법
- 신용정보관리·보호인 또는 신용정보 관리·보호 관련 고충을 처리하는 사람의 성명, 부서 및 연락처

- **(공시 방법)** 고객이 신용정보활용체제를 열람할 수 있도록 점포사무소 안의 보기 쉬운 장소에 갖추어두거나 인터넷 홈페이지를 통해 게시하여야 한다.

- **(개인신용정보 수집)** 개인신용정보 수집 시 신용정보법 또는 정관으로 정한 업무 범위에서 신용정보를 수집하고 처리목적을 명확화한다.

관련법령

- **신용정보법 제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존)** ①신용정보회사등은 신용정보의 수집·처리·이용 및 보호 등에 대하여 금융위원회가 정하는 신용정보 관리기준을 준수하여야 한다.

  ② 신용정보회사등은 다음 각 호의 구분에 따라 개인신용정보의 처리에 대한 기록을 3년간 보존하여야 한다.

  1~4.(생략)

- **(개인신용정보 처리 기록 보존)** 정보제공자와 정보수신자는 개인신용정보 처리에 대한 기록을 처리 구분(수집·이용, 제공, 폐기 등)에 따라 분류하여 기록이 발생한 날로부터 3년간 보존하여야 한다.

〈 개인신용정보 처리 방법에 따른 구분 〉

구분	항목
1. 개인신용정보를 수집·이용한 경우	가. 수집·이용한 날짜 나. 수집·이용한 정보의 항목 다. 수집·이용한 사유와 근거
2. 개인신용정보를 제공하거나 제공받은 경우	가. 제공하거나 제공받은 날짜 나. 제공하거나 제공받은 정보의 항목 다. 제공하거나 제공받은 사유와 근거
3. 개인신용정보를 폐기한 경우	가. 폐기한 날짜 나. 폐기한 정보의 항목 다. 폐기한 사유와 근거
4. 그 밖에 대통령령으로 정하는 사항	-

- **(개인신용정보 보관)** 정보제공자와 정보수신자는 금융거래 등 상거래 관계가 종료된 날부터 해당 고객의 개인신용정보가 안전하게 보호될 수 있도록 관리하여야 한다.

상거래 관계가 종료된 개인신용정보의 관리 방법

- 금융거래 등 상거래관계의 설정 및 유지 등에 필수적인 개인신용정보의 경우
  1. 상거래관계가 종료되지 아니한 다른 신용정보주체의 정보와 별도로 분리
  2. 접근권한 관리책임자를 두어 해당 개인신용정보에 접근할 수 있는 사람을 지정
  3. 접근권한을 부여받은 자가 해당 개인신용정보를 이용하려는 경우에는 접근권한 관리책임자의 사전 승인을 얻어 그 개인신용정보를 이용하게 하고, 그 이용내역을 3년간 보관
- 금융거래등 상거래 관계의 설정 및 유지 등에 필수적이지 않은 개인신용정보의 경우
  1. 해당 정보 모두 삭제

- **(개인신용정보 삭제)** 정보제공자는 금융거래 등 상거래관계가 종료된 날부터 최장 5년 이내(해당 기간 이전에 정보 수집·제공 등의 목적이 달성된 경우에는 그 목적이 달성된 날부터 3개월 이내)에 해당 고객의 개인신용정보를 관리대상에서 삭제하여야 한다. 마이데이터사업자는 고객의 개인신용정보 삭제 요청 시 또는 회원탈퇴 시 해당 고객의 개인신용정보를 관리대상에서 삭제하여야 한다.

관련법령

- **신용정보법 제38조의3(개인신용정보의 삭제 요구)** ① 신용정보주체는 금융거래 등 상거래 관계가 종료되고 대통령령으로 정하는 기간이 경과한 경우 신용정보제공·이용자에게 본인의 개인신용정보의 삭제를 요구할 수 있다. 다만, 제20조의2제2항 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

- **(개인신용정보 삭제 방법)** 개인신용정보 삭제 시, 보존매체의 특성을 고려하여 복구 또는 재생되지 아니하도록 하여야 한다.

〈 보존매체 특성에 따른 개인신용정보 삭제 방법 〉

보존매체 구분	삭제 방법
전자적 파일	현재 기술 수준에서 적절한 비용이 소요되는 방법으로서 복원이 불가능하도록 영구 삭제
인쇄물, 서면, 그 밖의 기록매체	파쇄 또는 소각

- **(개인신용정보를 삭제 할 수 없는 경우)** 현재 거래 중인 고객의 개인신용정보와 분리하는 등의 조치를 통해 안전하게 보관하고 해당 개인신용정보 활용 시 고객에게 통지하여야 한다.

개인신용정보를 관리대상에서 삭제하지 않는 경우

- 신용정보법 또는 다른 법률에 따른 의무를 이행하기 위하여 불가피한 경우
- 개인의 급박한 생명·신체·재산의 이익을 위하여 필요하다고 인정되는 경우
- 가명정보를 이용하는 경우로서 그 이용 목적, 가명처리의 기술적 특성, 정보의 속성 등을 고려하여 대통령령으로 정하는 기간 동안 보존하는 경우
- 예금·보험금의 지급을 위한 경우
- 보험사기자의 재가입 방지를 위한 경우
- 개인신용정보를 처리하는 기술의 특성 등으로 개인신용정보를 보존할 필요가 있는 경우

라. 개인신용정보처리 시스템 접근 관리

- **(내부 접근권한 관리)** 정보제공자와 정보수신자는 서비스 제공을 위하여 필요한 최소한의 인원에게만 개인신용정보를 처리할 수 있도록 개인신용정보처리시스템에 대한 접근권한 관리하여야 한다.

- **(내부 접근권한 부여)** 서비스 제공을 위하여 필요한 최소한의 인원에게만 개인신용정보 접근 권한을 직급별·업무별로 차등하여 부여하여야 한다.

- **(내부 접근권한 변경)** 정보제공자와 정보수신자의 지휘·감독을 받아 개인신용정보 업무를 처리하는 개인신용정보 취급자가 전보 또는 퇴직 등 인사이동으로 인하여 변경되었을 경우, 지체없이 개인신용정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.

- **(내부 접근권한 변경 기록)** 내부 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

- **(외부 접근권한 관리)** 업무목적을 위하여 불가피한 경우 외부사용자에게 개인신용정보처리 시스템에 대해 최소한의 접근 권한을 부여하고, 권한 부여에 관한 기록을 3년 이상 보관하는 적절한 통제시스템을 마련하여야 한다.

- **(외부 접속 보안)** 외부에서 개인신용정보처리시스템 접속 시 안전한 접속수단 또는 안전한 인증수단(VPN 등)을 적용하여야 한다.

- **(접속기록 관리)** 개인신용정보처리 시스템에 접속하여 개인신용정보를 처리한 경우 처리일시, 처리내역 등 접속 내역을 기록하여야 한다.

  - **(접속기록 확인·감독)** 저장된 접속기록을 월 1회 이상 정기적으로 확인·감독한다.

  - **(접속기록 백업)** 개인신용정보처리 시스템의 접속기록을 1년 이상 저장하고, 위변조되지 않도록 별도 저장장치에 백업 보관한다.

- **(비밀유지서약서 징구)** 정보제공자와 정보수신자는 개인신용정보처리 시스템 등에 접근하는 내·외부직원을 대상으로 정보보호비밀유지서약서를 징구하여야 한다.

  - **(작성 방법)** 정보보호에 대한 책임 및 준수사항을 포함하는 서류를 임직원 및 외부자의 서명과 함께 작성한다.

마. 직무분리

- **(직무분리 기준 마련)** 권한 오남용 등 고의적인 행위로 발생할 수 있는 잠재적인 피해를 줄이기 위하여 직무분리 기준을 마련한다.

  - **(직무분리 기준 수립)** 직무별 권한과 책임을 분산시켜 직무 간 상호견제를 할 수 있도록 직무별 역할과 책임을 명확하게 기술한다.

- **(직무분리 보완책 마련)** 인적자원 부족 등 불가피하게 직무분리가 어려운 경우 직무자간 상호 검토 등 별도의 보완책을 마련한다.

바. API 시스템 관리

- **(자격증명·접근토큰 관리)** 정보제공자와 마이데이터사업자는 자격증명 및 접근토큰을 안전하게 관리하고 위변조를 방지하기 위한 수단을 마련하여야 한다.

  - **(중복토큰 발급 확인)** 정보제공자는 접근토큰과 리프레시토큰 중복발급 방지를 포함하여 토큰이 안전하게 관리될 수 있는 수단을 마련하고 이를 주기적으로 확인하여야 하며, 마이데이터사업자는 정보제공자로부터 수신한 토큰의 중복발급 여부를 확인하고, 중복발급을 확인한 즉시 전송요청를 중지하여야 한다.

- **(중복토큰 발급 사실 확인 시 조치)** 정보제공자 및 마이데이터사업자는 중복토큰 발급 사실 확인시, 오전송되는 개인신용정보가 없도록 상호 협조하여야 한다.

- **(API 관련 시스템 보호)** 정보제공자는 API와 관련된 시스템에 방화벽, 침입탐지·차단 시스템, 망분리, 백신 소프트웨어 등 외부 공격 시도에 대한 방어 장치를 마련하여야 한다.

- **(비정상 API 탐지)** 정보제공자는 비정상적인 API 접근을 모니터링하고 필요 시 API의 접근 제한 등을 수행할수 있어야 한다.

- **(클라우드 이용)** 마이데이터사업자는 클라우드 이용시 전자금융감독규정 등 관련 법규에서 요구하는 사항을 만족하여야 한다.

관련법령

- **전자금융감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등)** ① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.
  1. 자체적으로 수립한 기준에 따른 이용대상 정보처리시스템의 중요도 평가
  2. 〈별표 2의2〉의 항목을 포함한 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등 평가
  3. 〈별표 2의3〉에서 정하는 사항을 반영한 자체 업무 위수탁 운영기준의 마련 및 준수

  ② 금융회사 또는 전자금융업자는 제1항에 따른 평가결과 및 자체 업무 위수탁 운영기준에 대하여 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

  ③~⑦ (생략)

  ⑧ 제2항의 절차를 거친 클라우드컴퓨팅서비스 제공자의 정보처리시스템이 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다. 다만, 금융회사 또는 전자금융업자(전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제대행업자는 제외한다)가 제3항제1호에 따른 고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.

  ⑨ (생략)

사. 이용자 보호

○ **(개인신용정보 누설)** 정보제공자는 개인신용정보가 업무 목적 외로 누설되었음을 알게 되었을 시, 서면, 전화, 전자우편, 휴대전화 문자메시지(SMS) 등을 통해 지체없이 해당 고객에게 통지하여야 한다.

개인신용정보 누설의 예

- 신용정보회사등이 개인신용정보에 대하여 통제를 상실하거나 권한 없는 자의 접근을 허용한 경우로서 아래의 예시 및 이와 유사한 경우 등에는 개인신용정보 누설로 볼 수 있음

1. 개인신용정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인신용정보가 저장된 데이터베이스 또는 개인신용정보처리시스템에 권한 없는 자가 접근한 경우
3. 신용정보회사등의 고의 또는 과실로 개인신용정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우

※ 출처 : 신용정보업감독규정 [별표 4-2] 신용정보 관리기준

관련법령

- **신용정보법 제39조의4(개인신용정보 누설통지 등)** ① 신용정보회사등은 개인신용정보가 업무 목적 외로 누설되었음을 알게 된 때에는 지체 없이 해당 신용정보주체에게 통지하여야 한다. 이 경우 통지하여야 할 사항은 「개인정보 보호법」 제34조제1항 각 호의 사항을 준용한다.

개인신용정보 누설 시 통지 사항

- 누설된 개인신용정보의 항목
- 누설 시점과 그 경위
- 누설로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
- 신용정보회사등의 대응조치 및 피해 구제절차
- 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

- 개인신용정보가 누설된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

○ **(1만명 이상의 개인신용정보 누설)** 1만명 이상의 고객에 관한 개인신용정보가 누설되었을 경우, 신용정보주체 통지와 더불어 추가적인 방법으로 신용정보 누설을 알려야한다.

1만명 이상의 개인신용정보 누설시 통지 사항

- 누설된 개인신용정보의 항목
- 누설 시점과 그 경위
- 누설로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
- 신용정보회사등의 대응조치 및 피해 구제절차
- 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

1만명 이상의 개인신용정보 누설시 통지 방법

1. 15일간 인터넷 홈페이지에 그 사실을 게시
2. 15일간 사무실이나 점포 등 해당 신용정보주체로 하여금 그 사실을 열람토록 조치
3. 7일간 주된 사무소가 있는 특별시·광역시·특별자치시·도 또는 특별자치도 이상의 지역을 보급지역으로 하는 일반일간신문, 일반주간신문 또는 인터넷 신문에 그 사실을 게재

- **(신고서 제출)** 1만명 이상의 고객에 관한 개인신용정보가 누설된 경우, 지체없이 금융위원회 또는 금융감독원에 “개인신용정보 누설신고서”(신용정보업감독규정 별지 제18호 서식)를 제출하여 신고하여야 한다.

  - 단, 신용정보 추가누설을 방지하기 위한 조치가 시급한 경우 해당 조치를 취한 후 지체없이 조치의 내용과 함께 신고서를 제출할 수 있다.

관련법령

- **신용정보법 제39조의4(개인신용정보 누설통지 등)** ③ 신용정보회사등은 대통령령으로 정하는 규모 이상의 개인신용정보가 누설된 경우 제1항에 따른 통지 및 제2항에 따른 조치결과를 지체 없이 금융위원회 또는 대통령령으로 정하는 기관(이하 이 조에서 "금융위원회등"이라 한다)에 신고하여야 한다. 이 경우 금융위원회등은 피해 확산 방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

- **신용정보법 시행령 제34조의4(개인신용정보의 누설사실의 통지 등)** ④ 법 제39조의4제3항 전단에서 "대통령령으로 정하는 규모 이상의 개인신용정보"란 1만명 이상의 신용정보주체에 관한 개인신용정보를 말한다.

  ⑤ 법 제39조의4제3항 전단에서 "대통령령으로 정하는 기관"이란 금융감독원을 말한다.

  ⑥ 법 제39조의4제3항 전단에 따라 신고해야 하는 신용정보회사등(상거래 기업 및 법인은 제외한다)은 그 신용정보가 누설되었음을 알게 된 때 지체 없이 금융위원회가 정하여 고시하는 신고서를 금융위원회 또는 금융감독원에 제출해야 한다.

  ⑦ 제6항에도 불구하고 제3항 전단에 해당하는 경우에는 우선 금융위원회 또는 금융감독원에 그 개인신용정보가 누설된 사실을 알리고 추가 유출을 방지하기 위한 조치를 취한 후 지체 없이 제6항에 따른 신고서를 제출할 수 있다. 이 경우 그 조치의 내용을 함께 제출해야 한다.

아. 재해·재난 대응 대비

○ **(백업 및 복구 시스템 운영)** 정보제공자와 마이데이터사업자는 개인신용정보처리시스템의 데이터 백업 시스템 및 재해·재난 침해사고 등 위협 발생 시 대응을 위한 복구 시스템을 설치·운영하여야 한다.

- **(백업·복구 대책 마련)** 사고 발생 시 개인신용정보처리시스템의 신속한 백업 및 복구를 위한 대책을 마련한다.

- **(재해·재난 대응 체계 수립)** 재해·재난 발생을 대비하는 비상계획, 재해복구 훈련 실시 체계를 수립한다.

5.3. 물리적 보안사항

가. 접근통제

○ **(전산설비 분리)** 개인신용정보처리시스템을 운영하는 장소는 물리적 보호구역으로 지정하여 운영하고, 물리적 접근 방지를 위한 출입통제시스템을 설치하여 수립된 출입통제 절차에 따라 출입하여야 한다.

※ 외부 공동전산시설(IDC)을 이용하는 경우 일정수준 이상*의 물리적·기술적 보호조치를 갖춘 시설을 이용할 것을 권고
* 정보보호 관리체계(ISMS, ISO27001 등) 인증을 득한 안전한 시설 이용 권장

※ 개인신용정보를 수집 관리하는 전산 설비는 국내에 위치하여야 한다.(단, 전자금융감독규정 제14조의2항에 따라 국외 사이버몰을 위한 전자지급결제대행업자에 대해서는 그렇지 아니하다.)

- **(출입내역 기록·관리)** 비밀번호 기반, 스마트카드 기반, 바이오정보 기반 등 출입통제 시스템을 설치·적용하고 출입 내역(출입자, 출입일시, 출입목적, 소속 등)을 기록·관리한다.

○ **(보조저장 매체 반·출입 통제)** 보조저장매체 사용 시 책임자 승인, 반·출입 내역 관리 등 통제 절차를 수립하고 적용한다.

- (보조저장매체 접근 통제조치) 개인신용정보처리시스템의 보조저장 매체 접근을 통제하는 보안통제방안*을 설치·운영한다.
  * 접근통제 소프트웨어, 보안스티커 부착, 물리적 봉인 등

- **(보조저장 매체 반·출입 기록 및 관리)** 보조저장매체를 사용할 경우 사용 목적, 일시, 담당자 승인 등 관련 내역을 세부적으로 기록하고 관리한다.

- **(외부자 출입 통제)** 제휴, 위탁 또는 외부주문에 의한 개인신용정보처리시스템 등의 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영한다.

나. 물리적 보안

- **(물리적 보안설비 구축)** 안전한 물리적 보안설비(통신회선 이중화, CCTV 등)를 갖추어야 한다.

- **(문서 보관)** 개인신용정보가 포함된 문서 등은 보존기간을 정하여 잠금장치가 있는 캐비넷 등 안전한 장소에 보관하며 열람, 대여 등에 관한 통제시스템을 확립하고 시행한다.

5.4. 기술적 보안사항

가. 비밀번호 관리

- **(비밀번호 관리)** 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자를 비밀번호로 이용하지 않도록 비밀번호 작성 규칙을 수립하고 이행한다.

예시 **비밀번호 작성 규칙 예시**

- 비밀번호는 문자, 숫자의 조합·구성에 따라 최소 10자리 또는 8자리 이상의 길이로 설정
  * 기술 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있다.
  - 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개), 특수문자(#, [, “, 〈 등, 32개) 중 2종류 이상으로 조합·구성한 경우

- 최소 8자리 이상 : 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성한 경우

• 비밀번호는 추측하거나 유추하기 어렵도록 설정
- 일련번호(12345678 등), 전화번호, 잘 알려진 단어(love, happy 등), 키보드 상에서 나란히 있는 문자열(qwer 등) 등을 사용하지 않도록 한다.

• 비밀번호를 최소 6개월마다 변경하도록 변경 기간을 적용하는 등 장기간 사용하지 않는다.
- 변경 시 동일한(예시 : Mrp15@*1aT와 Mrp15@*1at) 비밀번호를 교대로 사용하지 않도록 한다.

※ 출처 : 개인정보의 안전성 확보조치 기준 해설서

- **(비밀번호의 주기적 변경)** 각종 비밀번호는 정기적으로 변경하여야 하며 비밀번호 유효기간을 내부정책에 반영하고 시행·관리한다.

- **(비밀번호 차단 및 해제)** 비밀번호를 일정 횟수 이상 잘못 입력한 경우 해당 계정의 접속을 차단하고 본인 여부 확인을 내부정책 및 절차에 따라 실시하여야 하며, 접속 차단 및 해제 등의 이력을 기록·관리한다.

○ **(비밀번호 암호화)** 비밀번호(개인식별이 가능한 바이오 정보, 본인인증정보 등 포함)는 복호화되지 아니하도록 일방향 암호화하여 저장한다.

나. 암호 통제

○ **(개인신용정보 암호화)** 개인신용정보(고유식별정보, 비밀번호, 바이오정보 등 포함)를 암호화하여 저장한다.

〈 암호화 의무 적용 주요내용 〉

적용 기준	구 분	암호화 적용 기준
저장 시	비밀번호, 바이오 정보	• 암호화하여 저장하여 조회할 수 없도록 조치 – 조회가 불가피한 경우 조회사유·내용 등 기록·관리
	개인신용정보	• PC에 저장시 암호화
	주민등록번호	• 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 저장시 암호화 • 내부망에 주민등록번호 저장시 암호화 • 업무용 컴퓨터에 저장 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장
송·수신 시	개인신용정보, 비밀번호, 바이오 정보	• 정보통신망을 통한 송·수신시 SSL 또는 암호화 응용 프로그램 등을 이용하여 암호화
	주민등록번호	• 정보통신망을 통하여 송수신하거나 보조저장매체를 통하여 전달하는 경우 암호화
기타	개인신용정보 (개인식별정보)	• 신용정보집중기관과 신용조회회사가 서로 개인식별번호를 제공하는 경우, 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화 • 신용정보회사등이 개인신용정보의 처리를 위탁하는 경우 개인식별번호를 암호화하여 수탁자에 제공

※ 출처 : 금융분야 개인정보보호 가이드라인, 금융위원회(2016.12.)

– **(업무용 단말기 저장 시 암호화)** 업무용 단말기 및 모바일 기기에 개인신용정보를 저장할 경우 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화한다.

응용프로그램에서 제공하는 암호 설정 기능

- 한컴 오피스 : 파일〉〉다른 이름으로 저장하기〉〉문서 암호 설정에서 암호 설정
- MS 오피스 : 파일〉〉다른 이름으로 저장하기〉〉도구〉〉일반옵션에서 암호 설정
- 어도비 아크로뱃 : 고급〉〉보안〉〉암호로 암호화 또는 인증서로 암호화
- MS Windows 폴더(파일) 암호화 : 암호화 폴더(파일) 선택하고 마우스 오른쪽 버튼 클릭〉〉속성〉〉일반〉〉고급에서 암호 설정

※ 출처 : 개인정보의 안전성 확보조치 기준 해설서

- **(통신구간 암호화)** 정보통신망을 통해 개인신용정보 및 인증정보를 송·수신할 때에는 보안서버 구축 등의 조치를 통해 암호화하여야 한다.

※ 단 전용회선등을 통해 개인신용정보등을 전송할 시에는 그렇지 아니하다.

- **(안전한 TLS 인증서 적용)** TLS1.3 버전 이상의 인증서를 적용하여 인터넷 기반으로 개인신용정보를 암호화하여 송·수신한다.

참고

〈 TLS 이용 시 고려사항 〉

분류	설명
공신력 있는 인증서 이용	공신력 있는 인증기관에서 발급한 TLS 인증서 이용 * 신뢰성이 높고, 기관 정보를 확인할 수 있는 EV(Extended Validation) 등급 인증서 사용)
상호인증	양방향TLS(Mutual TLS)을 적용하여 상호인증 수행
최신 버전의 TLS 이용	TLS1.3 이상을 적용하며 최신 업데이트(패치)를 유지
안전한 암호 알고리즘 이용	안전한 데이터 교환을 위한 암호 알고리즘(암호화 키 교관, 메시지 인증, 데이터 암호화 등)을 이용
인증서 및 키 관리	인증서 및 데이터 전송·암호화에 이용되는 키를 안전한 방법으로 저장·관리
접근통제	TLS 설정 등에 접근 가능한 기기·사용자 등 접근통제 수행
보안에 취약한 옵션 미사용	재생공격에 취약한 0-RTT 핸드쉐이크 옵션 미사용

☞ TLS를 안전하게 사용하는 경우에 한하여 API기반 개인신용정보 전송구간에서는 전용선이나 공중인터넷망 사용이 가능하다. 단, 정보제공자가 금융회사인 경우 중계기관과의 연결시 반드시 전용선 및 이에 준하는 연결을 하여야 한다.

☞ 안전한 TLS이용을 위해 TLS1.3을 이용하여야 하며 내부 여건으로 하위버전(1.2등)를 이용하는 경우에는 가급적 신속하게 업데이트하여야 한다.

- **(암호키 관리)** 암호화 키가 접근이 인가된 사용자 외에는 노출되지 않도록 관리하며 생성부터 폐기까지의 관리기준을 수립하여 안전하게 관리한다.

  ※ 금융부문 암호기술 활용 가이드, 금융보안원, 2019.1. 참고

다. 시스템 보안

- **(망분리)** 내부 업무용시스템, 전산실 내 위치한 정보처리시스템과 해당 시스템에 직접 접속하는 단말기에 대해서 망분리를 수행한다.

  - **(내부 업무용시스템 망분리)** 내부통신망과 연결된 내부 업무용시스템 등은 외부통신망과 분리차단할 수 있도록 망분리를 수행하여야 한다.

  - **(정보처리시스템 망분리)** 전산실 내 위치한 정보처리시스템과 해당 정보처리시스템에 직접 접속하는 단말기에 대해서 인터넷 등 외부통신망으로부터 물리적으로 분리하여야 한다.

관련법령

- **전자금융감독규정 제15조(해킹 등 방지대책)** ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

  1.,2. (생략)

  3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)

  4. (생략)

  5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)

- **(침입차단·탐지시스템 설치 및 운영)** 개인신용정보처리시스템에 침입차단시스템과 침입탐지시스템을 설치하고 운영하여야 한다.

  - **(침해위협 탐지·대응)** 내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응한다.

  ※ 가입자 수 100만명 이상의 마이데이터사업자는 가입자 100만명에 도달한 시점에서 1년 이내에 금융보안원 금융보안관제센터가 제공하는 보안관제 서비스에 가입해야 한다.

  - **(이상거래 탐지 및 대응)** 이상거래 시도를 포함한 보안사고 등을 모니터링 및 기록(IP주소, 인증 실패 횟수, 부정한 API 요구 등)하고 지원기관에 공유한다.

- **(백신소프트웨어 설치·관리)** 개인신용정보처리시스템 등 정보처리기기에 컴퓨터 바이러스, 스파이웨어 등 악성 프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치한다.

  - **(백신소프트웨어 갱신·점검)** 소프트웨어는 월 1회 이상 주기적으로 갱신·점검하고, 바이러스 경보가 발령된 경우 및 백신 소프트웨어 제작 업체에서 업데이트 공지를 한 경우 즉시 최신 소프트웨어로 갱신·점검한다.

라. 개발 보안

- **(보안 설계)** 마이데이터서비스 개발 및 변경 시 보안 요구사항을 도출하고 이에 대한 대책을 설계에 반영하여 개발한다.

  - **(API보안 설계)** 자격증명, 접근토큰 등 API 관련 중요정보가 처리과정 및 관리과정 중 노출되지 않도록 설계하고 이에 따라 개발한다.

- **(테스트데이터 활용)** 마이데이터서비스 개발시에는 개인신용정보가 아닌 가상의 테스트데이터를 활용해야 한다.

○ **(취약점 점검)** 마이데이터사업자는 고객에 마이데이터서비스를 제공하기 이전에 취약점 점검을 수행하여야 한다.

※ 금융보안원 또는 전문기관을 통해 취약점 점검 수행

마. 출력·복사 시 보호조치

○ **(출력·복사 보호 내부시스템 구축)** 개인신용정보취급자는 개인신용정보 출력·복사 시 보호조치를 위한 내부시스템을 구축한다.

○ **(출력항목 최소화)** 개인신용정보처리 시스템에서 개인신용정보를 출력(인쇄, 화면표시, 파일생성 등)할 경우 용도를 특정하여야 하며, 불필요한 개인신용정보가 노출되지 않도록 출력 목적에 따라 출력 항목을 최소화한다.

- **(불필요 정보 마스킹·삭제 처리)** 불필요한 정보가 노출되지 않도록 일부 정보를 마스킹하거나 삭제한다.

○ **(출력·복사 시 기록·관리)** 개인신용정보를 조회(출력, 복사 등)하는 경우 조회자의 신원, 조회일시, 대상정보, 목적, 용도 등을 기록하고 관리한다.

○ **(외부 전송 사전 승인)** 개인신용정보를 보조저장매체에 저장하거나 이메일 등의 방법으로 외부에 전송하는 경우 관리책임자의 사전 승인을 받아야 하며, 승인신청자에게 관련 법령을 준수하여야 한다는 사실을 알려야 한다.