Privacy Report 2020.12

SOMANSA

데이터3법. 핵심은 보호와 활용의 균형

개 인정보 보호법 ⊃ 정 보통신망법 신 용 정보법

관련법 전 자금융거래법 온 라인투자 연계금융법

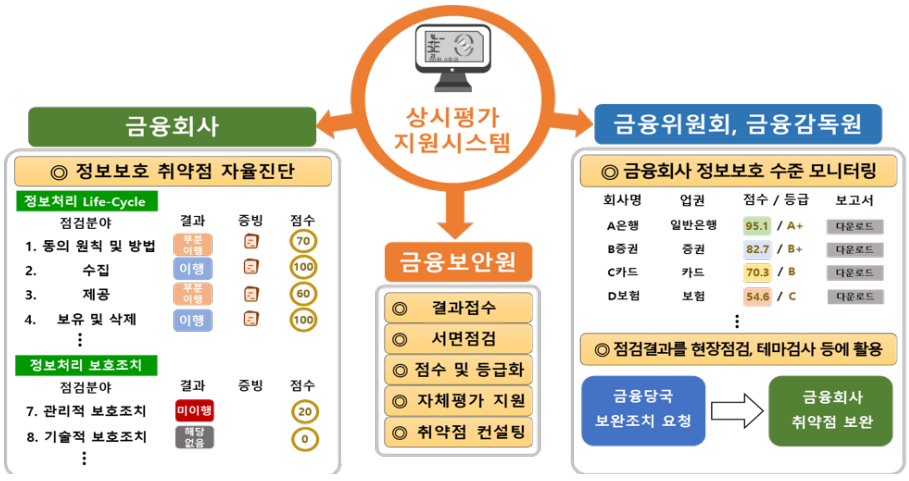
신 용 정보법 금융권 정보보호 상시평가제의 보호조치분석

금융권 정보보호상시평가제는 무엇인가?

배경	데이터3법 개정에 따라 금융기관의 보호수준 강화필요
평가대상	기존 모든 금융기관과 **마이데이터사업자**
평가 3 단계	① 가이드라인 9개대항목 143개 소항목 자체진단, **결과를 이사회에 보고** ② 금융보안원 온라인평가시스템에 제출, **금융보안원이 검토. 점수화하여 등급 산출** ③ 등급 미달시 금융당국 실사
기한	**2021년 3월31일까지** 2020년도 평가실태 제출

금융권 정보보호상시평가제의 4대 의미

1. 보안점검결과를 대표자 및 이사회에 매년 보고해야 함
2. 금융보안원이 모든 금융기관의 보안을 점수화하여 등급화
3. 대표이사가 〈정보〉 파기책임자
4. 데이터3법개정에 따라 가명정보보호조치 및 신용정보주체 권리보장 반영



신 용 정보법

한 페이지로 보는

정보보호상시평가제 가이드라인상 보호조치항목

1 (주민번호, 여권번호 , 운전면허번호, 외국인등록번호, 국내거소번호) 개인식별번호 5종, 저장 및 전송시 암호화

DB, 서버, 엔드포인트 , 보조저장매체 저장 및 전송시 암호화

2 신용정보관리보호인이 월 1회 이상 개인정보과다조회 통제, 접속기록 이상징후 점검

개인정보과다조회 통제기록, 신용정보관리보호인이 직접 월 1회 이상 대량조회, 정정, 다운로드, 삭제, 출력 등 이상행위 점검

접속기록에 Whose Privacy 포함
Whose privacy : 접속대상인 해당정보주체를 식별할수 있는 정보

3 개인정보 유노출 통제

개인정보처리시스템에서 〈정보〉 화면표시, 인쇄, 파일생성시 기록관리, 표시제한, 승인통제

〈정보〉를 이메일로 외부전송시 사전승인 시스템 을 거쳐야 함

〈정보〉를 보조저장매체 저장시 사전승인 시스템을 거쳐야 함

유해 사이트 (악성프로그램 유포지 등) 접속 차단

4 유효기간이 지난 〈정보〉의 파기

반드시 전자적증빙제출

대표이사가 파기책임자

상거래가 종료된 필수적 〈정보〉

저장위치	상거래종료~3개월	3개월~ 5년	5년 이상~
DB	접근권한분리	접근통제 강화, 별도DB 테이블로 분리 **〈증빙〉 반드시 DB조회쿼리제출**	정보 파기 **〈증빙〉 반드시 전자적 증빙제출**
PC 스마트단말 서버 (로그& 이미지파일)	정보 파기작업	정보 파기상태 유지	-
문서	**대표이사 확인항목임(책임자를 신용정보관리보호인 혹은 대표이사로 명시)**		

상거래가 종료된 비필수적 〈정보〉 파기완료

저장위치	상거래종료~3개월
DB PC 스마트단말 서버	정보 파기완료〈 **증빙〉 반드시 전자적증빙제출**

신 용 정보법 정보보호 상시평가제 가이드라인
9개 대항목, 143개 소항목

대항목1. 수집·처리
〈정보〉수집원칙 (2)
개인의 건강관련정보
수집 및 제공시 동의 (1)

대항목2 제공
〈정보〉
제공원칙 (2)
보안계약 (3)

대항목3 처리위탁
보안계약 체결 (1)
수탁자 대상
교육 및 감독(3)

대항목5 동의원칙 및 방법
정보활용동의고지 및 동의 원칙(4)
정보활용동의의 필수/선택적 동의 원칙(3)
정보활용 동의의 요약정보 제공 원칙 (2)
정보활용 동의등급 (1)

〈〈정보〉〉 기술적 보호조치 연관규정

대항목4 보유 및 삭제	대항목6 〈정보〉의 기술적 보호조치	대항목7 〈정보〉의 관리적 보호조치
	접근통제(4)	신용정보관리·보호인 (4)
상거래관계가 종료된 〈정보〉 접근통제 강화 (5)	접속기록의 위 · 변조방지 (10)	조회권한 구분 (4) 〈정보〉의 이용제한 등 (1)
상거래관계 종료에 따른 〈정보〉 삭제(4)	암호화 (11)	내부관리규정 수립 및 관리 (11)
분리보관 중인 〈정보〉 활용 시 통지(1)	컴퓨터 바이러스 방지(4)	〈정보〉 처리기록 보존(3)
	출력·복사시 보호조치(10)	
	취약점 점검 (2)	

데이터3법개정에 따른 신규 규정

대항목8 신용정보주체의 권리보장	대항목9 가명정보에 대한 보호조치
8.1. 신용정보활용체제 공시	
8.2. 〈정보〉 이용 및 제공사실의 조회	
8.3. 개인신용평점 하락가능성 등에 대한 설명의무 및 사전통지	정보집합물 결합 및 관리 (1)
8.4. 〈정보〉 제공·이용 동의 철회권	추가정보에 대한 보호조치 (4)
8.5. 〈정보〉 열람 및 정정청구권	가명정보에 대한 보호조치 (6)
8.6. 〈정보〉 조회사실의 통지 요청	관리적 보호조치(4)
8.7. 〈정보〉 삭제 요구권	
8.8. 〈정보〉 이동권	
8.9. 자동화평가 결과 권리보장	

대항목4. 보유 및 삭제 (5)
상거래관계가 종료된 〈정보〉에 대한 접근통제 강화 등 (5)
상거래관계 종료에 따른 〈정보〉 삭제(4)
분리보관 중인 〈정보〉 활용 시 통지

4. 1 상거래관계가 종료된 경우 필수적인 〈정보〉의 접근통제 강화

4. 1 상거래관계가 종료된 경우 필수적인 〈정보〉의 접근통제 강화			증빙자료
4.1.1 상거래 종료시 필수적인 〈정보〉의 접근통제 강화	분리보관하는지 확인	3개월이내 : 접근권한을 분리하는 등 보안통제를 강화하여 운영하는지 확인	분리보관 관리현황 화면 or 문서
		5년 이내 : 상거래가 종료된 필수〈정보〉는 접근권한이 강화된 별도의 DB or Table로 분리하여 관리, 1단계 접근권한보다 강화된 방식으로 엄격히 통제하여 운영하는지 확인	**전자적 형태로 한정DB 조회 쿼리 (일부마스킹처리) 및 결과화면**
	접근할 수 있는 임직원을 지정	접근할 수 있는 임직원 지정 현황을 확인	접근지정 신청 절차, 방법, 표준서식관련 화면 or 문서
		서비스별, 〈취급자〉업무, 역할 등에 따라 접근권한 분류별 지정 인원 현황을 확인	접근권한 지정 현황 화면 or 문서
	접근권한 관리책임자 지정	상거래관계가 종료된 필수적 〈정보〉 이용시 접근권한 전결권자의 사전승인을 득하는지 확인	관리책임자 지정 현황 화면 or 문서
	접근권한 관리책임자의 사전승인 후 이용	상거래관계가 종료된 필수적 〈정보〉 이용 시 접근권한 전결권자의 사전승인을 득하는지 확인	사전승인 신청 절차, 방법, 표준서식관련 화면 or 문서 사전승인현황화면 or 문서
	필수적 〈정보〉 이용내역을 3년간 보관	이용내역을 전자적 or 수기로 작성, 3년간 보관하는지 확인	이용내역 기록 보관 화면 or 문서
		이용내역에 포함되어야 할 항목 - 신청일/접근자의 신원/관리책임자의 신원 - **대상정보**/이용목적/ 이용내역	
4.1.2 상거래 관계가 종료된 경우 필수적인 〈정보〉가 포함된 문서 등의 관리	보존기간을 정하여 잠금장치가 있는 안전한 장소 등에 보관	상거래관계가 종료된 〈정보〉 문서의 관리대장 등을 통해 보존기간 및 물리적 보관 현황을 확인	물리적 보안통제가 적용된 장소 화면 or 문서 보관 현황 화면 or 문서
		내화금고 or 별도의 잠금장치 등을 통해 안전하게 보관하는지 확인	
	물리적 보관장소에 대하여는 출입 · 통제 절차를 수립 · 운영	상거래관계가 종료된 〈정보〉 문서를 보관중인 물리적 보관장소에 대하여 출입 · 통제 절차에 따른 출입관리 통제 장치 및 관리대장 등을 통해 현황을 확인	출입 · 통제관련 화면 or 문서
		출입 · 통제 내역(전자적 or 수기 관리대장)에 포함되어야 할 항목 - 출입 일시/출입자 신원/출입 목적/확인자	
	보존기간이 만료한 〈정보〉에 대한 안전한 폐기계획을 수립 · 시행하고 신용정보관리/ 보호인 또는 대표이사 또는 대표자가 폐기결과를 확인	폐기대상, 폐기 방법, 보존기간 등을 정의한 폐기계획이 수립되어 있는지 확인	폐기계획 보고서 폐기결과 보고서
		폐기결과를 신용정보관리 · 보호인 or 대표이사가 폐기결과를 확인하는지 점검 - 외부업체를 통해 폐기 시 폐기 확인서 징구 및 확인	
		폐기결과 내역에 포함되어야 할 항목 - 폐기대상/보존기한/폐기결과/폐기확인자 등	

4.2 상거래관계 종료에 따른 〈정보〉 삭제

4.2 상거래관계 종료에 따른 〈정보〉 삭제			증빙자료
4.2.1 상거래관계가 종료된 경우 금융거래 등 상거래관계 설정 및 유지 등에 필수적이지 않은 〈정보〉는 3개월 이내에 삭제	3개월 이내에 모두 삭제하고, 그 결과를 전결권자가 검토승인하고 있는지 확인	삭제결과 내역에 포함되어야 할 항목 - 삭제대상/ 보존기한/ 삭제결과/ 삭제확인자 등	**증빙은 전자적 형태로 한정**
4.2.2 상거래관계가 종료되어 분리보관하는 필수적 〈정보〉를 최장 5년 이내에 삭제	상거래관계가 종료되어 분리보관하는 필수적 〈정보〉를 최장 5년 이내에 〈정보〉를 삭제하는지 확인	삭제결과 내역에 포함되어야 할 항목 - 삭제대상/보존기한/삭제결과/삭제확인자 등	
		※ 삭제대상이 법 제20조의2 제2항 단서(삭제 예외사유)에 모두 해당되는 경우에는 "해당없음" 처리	

4.3 분리보관 중인 〈정보〉 활용 시 통지

4.3 분리보관 중인 〈정보〉 활용 시 통지		증빙자료
4.3.1 **삭제 예외사유에 해당하여 삭제하지 않고 분리보관 중인 〈정보〉를 활용하는 경우 해당 신용정보주체에게 통지**	법 제20조의2제2항 단서(삭제 예외사유)에 해당하여 삭제하지 않고 분리보관하는 현황을 검토하고, 그 결과를 전결권자가 검토 · 승인하고 있는지 확인 ※ 검토결과 보고서에 삭제 예외사유 관련 법적근거를 명시 (oo법 제oo조 제oo항 제oo호)	분리보관 현황관련 내부검토결과 보고서
	〈정보〉를 보존하여 활용하는 경우 해당 신용정보주체에게 통지하는 현황을 검토하고, 그 결과를 전결권자가 검토 · 승인하고 있는지 확인	통지현황관련 내부검토결과 보고서

대항목6. 〈정보〉의 기술적 보호조치
접근통제(4) 접속기록의 위변조방지 (10) 암호화 (11)
컴퓨터 바이러스 방지(4) 출력·복사시 보호조치(10)
취약점 점검 (2)

6.1 접근통제

6.1 접근통제			증빙자료
6.1.1 〈시스템〉 접근권한을 최소인원에게 부여	〈시스템〉 현황관리	계정계,정보계 ,인터넷뱅킹, HTS, CRM 등으로 분류	〈시스템〉 현황 화면 or 문서
		업무용컴퓨터에 DB접속프로그램 설치 · 운영시 〈시스템〉에 해당	
	〈취급자〉 현황관리	〈정보〉를 처리하는 **모든** 인원을 〈취급자〉로 지정→관리 ※ 임직원, 파견 근로자, 시간제 근로자 등 포함	〈취급자〉 현황 화면 or 문서
		부서 or 업무별 현황, 대형사인 경우 지역별, 본부별 등으로 요약	
	접근권한 최소인원 부여	서비스, 업무, 직무, 역할에 따라 접근권한 부여인원 현황 확인	접근권한 부여현황 화면 or 문서
6.1.2 〈취급자〉 인사이동시 지체없이 권한변경 or 말소	퇴사 · 전보 발생 내역 확인		접근권한 변경말소 관리현황 화면 or 문서
	접근권한 변경 · 말소 처리에 따른 〈취급자〉 현황 확인		
6.1.3 권한부여, 변경, 말소내역(①,②)을 기록 최소 3년보관	접근권한 처리기록(전자적 or 수기)을 3년간 보관하는지 확인		접근권한처리 기록보관 화면 or 문서
6.1.4 〈시스템〉에 침입차단& 탐지시스템 설치운영	설치 · 운영	IDC or 클라우드 경우 침입차단/탐지시스템 사용계약현황 확인	침입차단, 탐지시스템 설치운영현황 화면 or 문서
	불법적침입 시도탐지대응	〈시스템〉 보안관제결과 점검 → 전결권자가 검토 · 승인 여부확인	보안관제 현황 보고서
		보안관제 탐지내용 분석 및 대응 (이상징후 발견 시 조치 등)	
6.1.5 ⑤ 〈정보주체〉 및 〈취급자〉 대상 PW 작성규칙 수립 &이행	생성규칙	영문, 숫자, 특수문자 중 3종류 이상 조합시, 8자리 /2종류 이상 조합시 10자리/ 생일, 주민번호, 전화번호, 연속숫자, 아이디와 비슷한 PW, 추측하기 쉬운 숫자 등은 제외	PW 생성 규칙 설정 화면
	주기적 변경	PW를 분기별 1회 이상 변경하는지 확인	PW주기적 변경 설정 화면
	오입력 잠김	PW 연속 오입력(5회 이내)시 즉시 잠김처리	PW 오입력 잠김 설정 화면
	〈시스템〉 접속프로그램 PW로 한정(없는 경우 시스템계정)		
6.1.6 〈정보〉 유노출 방지 방안 마련	기술적 방안	**1) 공유폴더 사용 통제**	유노출 방지 방안 적용 화면 or 문서
		2) 보조저장매체 사용 통제	
		3) 네트워크 기반 정보보호시스템 or 단말기 보안 프로그램을 통해 유해 사이트(악성프로그램 유포지 등) 접속 차단	
	관리적 방안	1) 단말기 보안점검 절차 등을 수립	
		2) 정기적으로 이행 실태를 점검	
6.1.7 제휴, 위탁 또는 외부주문 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치운영	전산설비 분리확인	개발/테스트시스템과 운영시스템을 분리설치 · 운영	외부주문 개발업무관련 보안관리 지침 문서
		개발/테스트 시스템과 운영시스템간의 접근통제 실시	
	사무실 분리확인	제휴, 위탁 or 외부주문 개발 사무실 위치 및 물리적 통제적용여부를 확인	
6.1.8 불가피한 경우에만 외부자에게 〈시스템〉접근권한을 부여 관련기록을 3년 보관	전자기록 or 수기기록하고 기록을 3년간 보관하는지 확인		외부사용자에 대한 접근권한 처리기록 보관 화면 or 문서
	신청자 정보, 신청일시, 승인자 및 발급자 정보, 신청 및 발급 사유 등 발급 과정과 이력 등을 확인할 수 있도록 필요한 정보를 보관		

6. 2 접속기록의 위 · 변조방지

6. 2 접속기록의 위 · 변조방지				증빙자료
6.2.1 〈시스템〉에 대한 접속기록 관리	〈시스템〉 접속기록 (필수항목 포함)을 1년 이상 저장	필수항목	계정정보, 접속일시, IP , 수행업무, **처리한 정보주체정보**	접속기록 보관 화면 or 문서
	접속기록을 월 1회 이상 정기적으로 확인감독	**월1회 이상 접속기록을 통해 이상행위 (대량의 〈정보〉 조회, 정정, 다운로드, 삭제, 출력 등)를 점검** → 결과를 전결권자가 검토 · 승인하고 있는지 확인		
6.2.2 별도 저장장치에 백업	〈시스템〉 접속기록 백업 현황을 확인			백업절차, 방법문서 백업화면or 문서

6.3 암호화

6.3 암호화					증빙자료
6.3.1 PW, 바이오정보 등 〈인증정보〉	저장시 안전한 암호 알고리즘 적용 여부 확인	PW	일방향 암호알고리즘		암호 알고리즘 적용현황 화면o문서
		바이오정보	양방향 암호 알고리즘		
		그외	안전한 암호 알고리즘 적용		
6.3.2 〈인증정보〉의 조회가 불가피하다고 인정되는 경우 조회사유/내용기록/관리	불가피하게 〈인증정보〉조회시 관련 기록 여부 확인	필수정보	신청일, 신청자, 승인자, 조회목적, 조회내역		조회신청 현황 문서
6.3.3 정보통신망으로 〈정보〉 및 〈인증정보〉 송 · 수신시 보안서버 구축 등으로 암호화	〈정보〉, 〈인증정보〉 전송시 암호화	웹서버에 SSL인증서를 설치			암호화 적용 화면 or 문서
		웹서버에 암호화 응용프로그램을 설치			
6.3.4 〈정보〉를 PC저장시 암호화	일반적 조치	**상용암호화SW를 통한 자동암호화**			
	최소한의 조치	문서 PW, 압축시 PW 설정 등 수동암호화하여 정기적점검			
6.3.5 개인식별정보의 암호화 — 1. 정보통신망, 보조저장매체로 전달시 암호화	정보통신망으로 〈개인식별번호〉 송수신시 암호화	웹서버에 SSL인증서를 설치			
		웹서버에 암호화 응용프로그램을 설치			
	보조저장매체로 〈개인식별번호〉전달시 암호화				
2. DMZ저장시 암호화	**〈개인식별번호〉를 인터넷 및 DMZ 구간에 저장시 상용암호화 SW or 안전한 암호알고리즘으로 암호화하는지 확인**				
3. 내부망에 〈개인식별번호〉 저장시 암호화	〈개인식별번호〉를 내부망저장시 상용암호화 SW or 안전한 암호알고리즘을 사용하여 암호화 하는지 확인				
4. 업무용컴퓨터 or 모바일 저장시 **상용암호화 SW or 안전한 알고리즘으로 암호화**	기술적	암호화관련소스코드나 암호화를 적용한 상용 SW			
	관리적	문서편집 SW의 PW 설정, 압축시 PW 설정 등의 방법으로 수동암호화하며 정기적으로 이행실태 점검			
5. 〈개인식별번호〉를 암호화하여 수탁자에게 제공	전자파일 경우	전자파일을 정보통신망 or **보조저장매체를 통하여 제공하는 경우 암호화하여 제공하는지 확인**			
	종이문서 경우	종이문서로 제공하는 경우 봉함하여 제공하는지 확인			

6.4 컴퓨터 바이러스 방지

6.4 컴퓨터 바이러스 방지			증빙자료
6.4.1 〈시스템〉 및 〈취급자〉PC에 백신 설치	〈시스템〉 및 〈취급자〉 PC에 백신 설치 및 운영 여부 확인	중앙관리솔루션으로 백신 설치 및 운영을 확인 중앙관리솔루션이 없는 경우, 백신를 개별적설치, 주기적 설치 여부 점검을 하는지 확인 〈시스템〉 OS가 유닉스, 리눅스, Apple Mac OS 등 백신 설치가 제한되는 OS는 제외	백신 설치 현황 화면 or 문서
6.4.2 백신을 월 1회 이상 업데이트 및 현황 점검	〈시스템〉, PC의 백신을 월1회 이상 주기적으로 업데이트 (긴급업데이트 포함) 하고 점검하는지 확인	바이러스 경보가 발령된 경우 및 백신 제작 업체에서 업데이트 공지를 한 경우에는 즉시 최신 업데이트 및 점검	월별 백신 업데이트 점검 결과 문서

6.5 출력/복사시 보호조치

6.5 출력/복사시 보호조치				증빙자료
6.5.1 〈시스템〉에서 〈정보〉 출력시 (인쇄, 화면표시, 파일생성 등) 용도특정 및 용도에 따라 출력 항목 최소화	〈시스템〉을 통한 화면표시, 인쇄, 파일생성 등의 출력시 해당목적 달성을 위해 반드시 필요한 최소한의 〈정보〉가 출력되도록 보안대책을 마련하고 있는지 확인	**화면표시**	**기록관리 or 마스킹**	〈정보〉 출력 항목 최소화를 위한 보안대책이 포함된 문서
		인쇄	**인쇄승인 or 기록관리 or 워터마킹**	
		파일생성	**파일생성 최소화 or 파일생성시 기록관리, 승인**	
6.5.2 〈정보〉를 조회(활용) 하는 경우 기록 관리	조회기록을 관리하는지 확인	포함항목	조회자의 신원, 조회일시, **대상정보,** 목적, 용도 등	**전자적증빙인 경우 DB 조회 쿼리 및 결과 화면**
6.5.3 **〈취급자〉가 〈정보〉를 외부에 전송하는 경우 보호조치**	**관리책임자의 사전승인 처리 현황**	**〈취급자〉가 〈정보〉를 보조저장매체에 저장시 사전승인을 받는지 확인**		사전승인 현황 화면 or 문서
		〈취급자〉가 〈정보〉를 이메일 등의 방법으로 외부전송시 사전승인을 받는지 확인		
		외부전송 사전승인을 위한 내부시스템을 구축 및 운영하는지 확인		
	사전승인시 승인신청자에게 법령의 준수여부를 안내하고 주지시키는지 확인			사전승인 신청시 고지관련 사항이 포함된 화면 or 문서

6.6 취약점점검

6.6 취약점점검		증빙자료
6.6.1 〈개인식별번호〉 처리시 홈페이지 취약점 점검 실시 연1회 이상	**홈페이지를 통해 〈개인식별번호〉가 유출 · 변조 · 훼손되지 않도록 연1회 이상 취약점 점검을 실시→전결권자가 검토 · 승인하고 있는지 확인**	취약점점검결과 보고서
	주민등록번호,여권번호,운전면허의 면허번호,외국인등록번호로 한정함	
6.6.2 〈개인식별번호〉 처리 시 인터넷 홈페이지에 대해 실시한 취약점 점검 결과 보완조치	연1회 이상 취약점 점검을 실시한 취약점 점검결과에 대한 보완(이행)조치 결과를 전결권자가 검토 · 승인하고 있는지 확인	취약점 보완(이행) 조치 보고서

대항목7. 〈정보〉의 관리적 보호조치
신용정보관리·보호인 조회권한 구분 의 이용제한 등
내부관리규정 수립 및 관리 〈정보〉 처리기록 보존

7.2 조회권한 구분 (신용정보 관리보호인 책임사항)

7.2 〈정보〉의 조회권한 구분		증빙자료
7.2.1 〈정보〉 조회 권한을 직급별 · 업무별 차등 부여	〈취급자〉 직무, 역할 등에 따라 조회권한부여 현황을 전결권자가 검토 · 승인하고 있는지 확인	
7.2.2 〈취급자〉의 〈정보〉 취급현황을 확인할 수 있는 수단 및 이의 점검 · 감사체제 정비	〈취급자〉의 취급현황, 감사체제, 과다조회 기준 점검 · 감사 절차 수립 및 수행 관련하여 **연 1회이상 점검(감사)**한 내역을 전결권자가 검토 · 승인하고 있는지 확인	〈정보〉 취급현황 점검 및 감사 문서
7.2.3 〈정보〉 이상과다조회 부서 및 직원 등에 대해 점검 실시	이상 과다조회 기준에 따른 정기점검을 실시하고, 그 결과를 전결권자가 검토 · 승인하고 있는지 확인	과다조회 현황관련 내부점검결과 보고서
	조회 권한을 초과하여 조회를 **일정횟수 이상 시도**한 직원에 대한 통제 장치를 마련하고 적용	
	영업점 및 신용정보 관리부서의 〈정보〉 조회 건수에 대해 **월 1회 이상** 정기적으로 점검하고 조회건수가 평소보다 급증한 부서 및 직원들을 샘플링하여 점검 실시	
7.2.4 〈취급자〉가 입력하는 조회사유의 정확성 등 신용조회기록의 정확성을 점검	〈정보〉 조회기록(조회자의 신원, 조회일시, 대상정보, 목적, 용도 등)의 적정성을 점검하고, **그 결과를 〈신용정보관리보호인〉이 이 검토 · 승인**하고 있는지 확인	조회기록 적정성 점검결과 보고서

7. 3 〈정보〉 이용제한 등

7.3 〈정보〉의 이용제한 등			증빙자료
7.3.1 신용평가모형 또는 위험관리모형을 개발하는 경우 〈정보〉의 이용제한 보안대책을 준수	〈정보〉를 이용한 위탁 개발 및 시험시 실데이터 사용을 제한하고 있는지 점검하고, 그 결과를 전결권자가 검토 · 승인하고 있는지 확인	〈정보〉가 개발 시험과정에서 유출되는 것을 방지하기 위하여 시험데이터는 임의의 데이터를 생성하거나 운영데이터를 가공 · 변환한 후 사용하고 있는지 확인	〈정보〉의 이용제한 관련 보안대책 지침문서 〈정보〉의 이용제한 현황관련 내부 점검 결과 보고서
		실 〈정보〉 사용 금지 (다만, 개인신용평가회사, 개인사업자신용평가회사의 경우, 실 〈정보〉를 사용하지 않으면 모형 개발 or 검증 등이 불가능한 불가피성이 인정되면 사용 가능)	
		개발 위탁 시 〈정보〉 제공 금지 (불가피한 경우 변환하여 제공하고 개발 완료 즉시 삭제)	

7.5 〈정보〉 처리기록 보존 (신용정보관리보호인 책임사항)

7.5 〈정보〉 처리기록 보존			증빙자료
7.5.1 〈정보〉의 처리에 대한 기록을 3년간 보존	수집 · 이용한 기록을 3년간 보관	이용기록 내역에 포함되어야 할 항목 – 수집이용한 날짜, 정보의 항목, 사유와 근거	수집 · 이용한 기록 보관 화면 또는 문서
	제공하거나 제공받은 기록을 3년간 보관	제공기록 내역에 포함되어야 할 항목 – 제공한 날짜, 정보의 항목, 사유와 근거 – 제공받은 날짜, 정보의 항목, 사유와 근거	제공한 기록 보관 화면 또는 문서 제공받은 기록 보관 화면 또는 문서
	파기기록을 3년간 보관	파기기록 내역에 포함되어야 할 항목 – 파기한 날짜/정보의 항목/파기한 사유와 근거	파기한 기록 보관 화면 또는 문서

대항목8. 가명정보의 보호조치
정보집합물 결합 및 관리 (1) 추가정보에 대한 보호조치 (4)
가명정보에 대한 보호조치 (6) 관리적 보호조치(4)

8.8 〈정보〉 이동권

8.8 〈정보〉 이동권		증빙자료
8.8.1 신용정보주체의 〈정보〉 전송요구 보장	본인의 〈정보〉를 신용정보제공 · 이용자등에게 전송하여 줄 것을 요청할 수 있는 방법을 제공하는지 확인	· 전송요구 요청화면 또는 방법관련 안내문서 · 전송요구 요청/처리 현황 화면 또는 문서
	〈정보〉 전송시 정보처리장치로 처리가 가능한 형태로 전송하고 있는지 확인	
8.8.2. 신용정보주체의 〈정보〉 전송요구 철회보장	〈정보〉 전송 요구 철회를 위한 방법을 제공하는지 확인	· 전송요구 철회 요청화면 또는 방법관련 안내문서 · 전송요구 철회 요청/처리 현황 화면 또는 문서

8.9. 자동화 평가 결과 권리보장

8.9. 자동화 평가 결과 권리보장			증빙자료
8.9.1 자동화 평가 결과에 대한 설명 및 이의제기 권리보장	자동화 평가 결과에 대한 개인인 신용정보주체의 설명 요구 및 이의제기를 보장	자동화 평가 결과에 대한 설명 요구 및 이의 제기 보장 방법을 제공하는지 확인 – 자동화평가에 대한 설명 요구/처리 현황 확인 – 자동화평가에 대한 이의제기 요구/처리 현황 확인	· 설명 및 이의제기 요청화면 또는 방법관련 안내문서 · 설명 및 이의제기 요청/처리/통지 현황 화면 또는 문서
	개인인 신용정보주체의 자동화 평가 결과관련 설명 또는 이의제기 요구를 거절할 경우 거절의 사유 및 근거 통지	자동화 평가 결과에 대한 설명 및 이의제기 요청을 거절할 경우 거절의 사유 및 근거를 통지하고 있는지 확인	

대항목9. 가명정보의 보호조치

정보집합물 결합 및 관리 (1) 추가정보에 대한 보호조치 (4)
가명정보에 대한 보호조치 (6) 관리적 보호조치(4)

대항목9. 가명정보의 보호조치				증빙자료
9.1. 정보집합물 결합 및 관리	제3자의 정보집합물과 결합시 〈데이터전문기관〉을 통하는지 확인	포함내역	건별현황(의뢰일자, 제공건수, 제공받은 건수, 결합된 결과건수)이 포함	결합의뢰 현황 화면 or 문서
		작성기준	직전 연도말까지 〈데이터전문기관〉으로부터 결합의뢰에 대한 결과를 제공받은 실적	
9.2. 추가정보에 대한 보호조치	추가정보를 보존하는 경우 가명정보와 분리된 저장소에 암호화저장하는지 현황검토 결과를 전결권자가 검토승인하고 있는지 확인	접근권한이 강화된 별도DB or Table로 관리하는지 확인		분리보관 현황관련 내부검토결과 보고서 암호화적용 화면 or 문서 추가정보 현황 화면 or 문서
		가명처리안내서의 추가정보 예시 : 필요시 가명(해시값)과 원본 식별자와의 매핑테이블을 생성 · 보관할 수 있으며 이때 사용한 솔트값 or 키값, 해시값 생성규칙, 매핑 테이블 등이 추가정보에 해당		
	〈가명정보취급자〉의 추가정보 접근권한에 대한 관리책임자의 사전승인	가명정보취급자의 추가정보 접근이 불가피한 경우 전결권자의 사전승인을 득하여 일시적으로 부여하는지 확인		사전승인 현황 화면 or 문서
	추가정보 접근시 사전승인 기록 3년간 보관	필수항목	- 접근자의 신원/전결권자의 신원	기록 보관 화면 or 문서
			- 접근일시/대상정보/조회가 불가피한 사유/용도	
			- 접근 허용 기간	
	추가정보가 가명정보를 재식별하는 데 사용되는 등 부정한 목적으로 사용되지 않도록 월 1회 이상 주기적으로 점검	추가정보 접근내역 기록을 월 1회 이상 점검을 실시하고, 그 결과를 전결권자가 검토 · 승인하고 있는지 확인		월별 점검 현황 보고서
9.3 가명정보에 대한 보호조치	원본과 가명정보를 분리저장현황검토 →결과를 전결권자가 검토 · 승인	접근권한이 강화된 별도의 DB or Table로 관리하는지 확인		분리보관 현황관련 내부검토 결과보고서 분리보관 현황 화면 or 문서
	가명정보취급자 별도지정, 접근권한을 구분하여 운영	- 접근권한 분류 현황		가명정보 접근권한 부여 관리화면 or 문서
		- 접근권한별 지정 인원 총인원 (대형사인경우 지역별, 본부별 등으로 요약 가능)		
	가명정보를 취급하는 직원의 원본정보 접근권한에 대한 관리책임자의 사전승인	가명정보를 취급하는 직원이 원본정보 접근이 불가피한 경우 전결권자의 사전승인을 득하여 일시적으로 부여하는지 확인		사전승인 신청 절차, 방법, 표준서식관련 화면 or 문서 사전승인 현황 화면 or 문서
	원본정보 접근시 사전승인 기록 3년이상 보관	- 접근자의 신원/전결권자의 신원 - 접근일시/대상정보/조회가 불가피한 사유/용도 - 접근 허용 기간		기록 보관 화면 or 문서
	가명정보처리기록을 가명정보 파기 후 3년이상 보관하는지 확인	가명정보의 구체적인 처리 목적, 처리 방법, 처리 일시를 기록		파기된 가명정보 처리기록 보관 화면 or 문서
	가명정보 처리기록에 대해 월 1회 이상 주기적으로 확인 · 감독	가명정보 처리기록을 통해 가명정보 오남용에 대한 자체 제재기준에 따른 현황을 월1회 이상 점검하고, 그 결과를 전결권자가 검토 · 승인하고 있는지 확인		월별 점검현황 보고서

정보보호상시평가제 가이드라인			
9. 4 관리적 보호 조치	가명정보 및 추가정보에 접근하는 취급자들에 대해 가명정보보호교육을 연 1회 이상 수행	교육 결과 보고서	연 1회 이상 교육을 실시하고, 그 결과(교육 이수자, 미이수자 현황 포함)를 전결권자가 검토 · 승인하고 있는지 확인 – 교육계획을 수립하는지 확인 – 교육실시 후 미이수자 등을 관리하는지 확인
	가명정보의 보존기간을 주기적으로 검토하고, 그 적정성 여부를 판단하여 필요시 조정	가명정보의 보존기간 적정성 검토 및 조치관련 문서	가명정보의 보존기간을 주기적으로 검토하고 필요시 조정하는지 확인 〈보존기간 산정 기준(영 §17조의2③〉 1. 추가정보 및 가명정보에 대한 관리적 · 물리적 · 기술적 보호조치 수준 2. 재식별시 정보주체에 미치는 영향 3. 가명정보의 재식별 가능성 4. 가명정보의 이용목적 및 그 목적 달성에 필요한 최소기간– 접근권한별 지정 인원 총인원 (대형사인경우 지역별, 본부별 등으로 요약 가능)
	가명정보가 재식별된 경우 회수 및 삭제	가명정보를 이용하는 과정에서 특정 개인을 알아볼 수 있게 된 경우(재식별) 즉시 그 가명정보를 회수하여 처리를 중지하고, 특정 개인을 알아볼 수 있게 된 정보는 즉시 삭제하고, 그 결과를 전결권자가 검토 · 승인하고 있는지 확인	
	〈정보〉를 가명처리나 익명처리를 한 경우 조치기록을 3년간 보존	〈정보〉를 가명처리 or 익명처리한 조치기록 사항(법§40의2⑧각 호)을 3년간 보존하는지 확인 조치기록 내역에 포함되어야 할 항목 – 가명처리(or 익명처리)한 날짜/정보의 항목/사유와 근거	

(주)소만사 서울특별시 영등포구 영신로220 knk디지털타워 9층
Tel: 02 2636 8300 | Fax: 02 2636 8181 | Email: privacy@somansa.com