금융분야 가명·익명처리 안내서

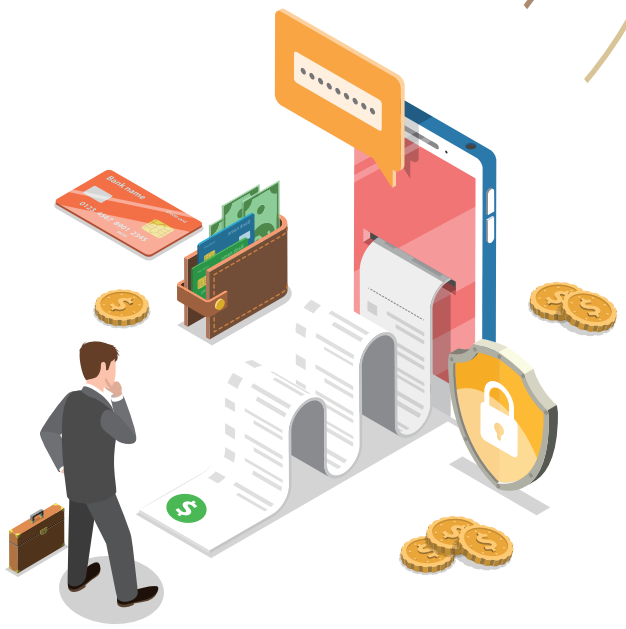
2022. 01.

금융위원회

금융감독원
FINANCIAL SUPERVISORY SERVICE

금융분야
가명·익명처리
안내서

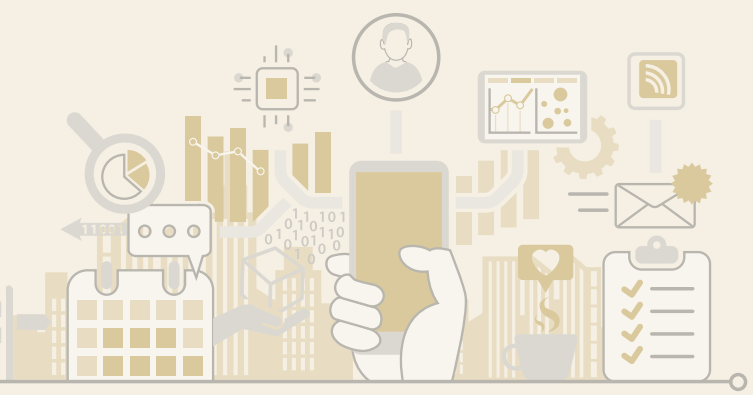
2022. 01.



금융위원회

금융감독원
FINANCIAL SUPERVISORY SERVICE

금융분야 가명·익명처리 안내서



Ⅳ. 정보집합물 결합

본 안내서는
개정 신용정보법 시행령 및 감독규정(2022년내 시행 예정)
관련 내용을 추가 반영할 예정으로,
최신 안내서는 금융위원회 홈페이지(www.fsc.go.kr) 또는
금융감독원 홈페이지(www.fss.or.kr)를 참고

Ⅰ. 개 요

Ⅰ. 개 요

1. 추진배경 및 목적

가. 추진배경

'20.8.5일 데이터 3법* 시행에 따라 가명정보, 익명정보를 법에 근거하여 활용할 수 있는 길이 열렸다. 이로 인해 은행 · 카드 · 보험 · 금융투자 등 금융업권 별로 체계적으로 관리되는 정형데이터와 통신정보 · 위치정보 · 보건의료정보 등 다른 산업분야에서 관리되고 있는 다양한 형태의 데이터를 서로 융합하여 금융분야의 혁신성장을 이끌 수 있게 되었다.

* 「개인정보 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 「정보통신망법」), 「신용정보의 이용 및 보호에 관한 법률」(이하 「신용정보법」)

개정된 「신용정보법」은 금융분야에서 기존 『개인정보 비식별 조치 가이드라인』(2016.7.1.시행)의 법적 한계를 극복하고 가명 · 익명처리한 정보를 안전하게 활용할 수 있는 제도적 기반을 마련하였다. 개정법에서는 통계작성(시장조사 등 상업적 목적의 통계작성 포함), 연구(산업적 연구 포함), 공익적 기록보존 등을 위하여 개인인 신용정보주체의 동의 없이 개인신용정보를 가명처리 하여 사용할 수 있을(「신용정보법」 제32조의2제6항 제9의2호)뿐만 아니라, 누구인지 알아 볼 수 없도록 익명처리한 경우에는 목적 제한 없이 자유로운 활용도 가능하게 되었다(「신용정보법」 제40조의2제4항).

본 안내서는 개정 「신용정보법」, 동법 시행령 및 하위 규정에 따른 가명 · 익명처리 및 활용에 대한 하나의 예시를 제시하여, 가명 · 익명처리에 대한 이해도를 높이고 가명정보 · 익명정보의 안전한 활용을 돕기 위해 마련하였다.

나. 목적

본 안내서는 신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관 및 신용정보제공 · 이용자(이하 '신용정보회사등')가 개인신용정보를 가명처리 또는 익명처리할 때 참고할 수 있는 사항을 안내하는 것을 목적으로 하며, 본 안내서에서 언급하지 않거나 안내서와는 다른 내용이더라도 가명 · 익명처리시 필요한 경우 관련법령을 준수하는 범위 내에서 신용정보회사등이 자체적으로 판단하여 활용할 수 있다. 본 안내서가 금융분야의 산업적 특성, 금융업권별 처리 정보의 특성 등을 고려하여 개인정보 자기결정권을 보장하고 금융산업 및 금융분야 정보산업의 발전에 기여할 수 있을 것으로 기대한다.

다. 적용범위

신용정보회사등이 개인신용정보를 가명·익명처리하거나 정보집합물 결합을 수행할 때 「신용정보법」, 「개인정보 보호법」 및 관계법령에 특별한 규정이 있는 경우를 제외하고는 본 안내서를 참고할 수 있다. 안내서의 내용과 법령이 상충될 경우 해당 법령에 따른다.

2. 용어정의

본 안내서에서 사용하는 용어의 뜻은 다음과 같다.

가. 개인신용정보

기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 신용정보로서 다음의 어느 하나에 해당하는 정보를 말한다(「신용정보법」제2조제2호).

1) 해당 정보의 성명, 주민등록번호 및 영상 등을 통하여 특정 개인을 알아볼 수 있는 정보
2) 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보

◎「**신용정보법**」 **제2조(정의)** 1. "신용정보"란 금융거래 등 상거래에서 거래 상대방의 신용을 판단할 때 필요한 정보로서 다음 각 목의 정보를 말한다.

가. 특정 신용정보주체를 식별할 수 있는 정보(나목부터 마목까지의 어느 하나에 해당하는 정보와 결합되는 경우만 신용정보에 해당한다)

나. 신용정보주체의 거래내용을 판단할 수 있는 정보

다. 신용정보주체의 신용도를 판단할 수 있는 정보

라. 신용정보주체의 신용거래능력을 판단할 수 있는 정보

마. 가목부터 라목까지의 정보 외에 신용정보주체의 신용을 판단할 때 필요한 정보

나. 속성(attribute)

속성이란 데이터의 고유한 특성을 말하며, 다음과 같이 구분된다.

1) 식별자

주민등록번호, 이메일주소, 휴대전화번호 등과 같이 그 자체로 특정 개인을 직접 식별하는 용도로 사용하는 속성을 말한다.

2) 개인식별가능정보

연령, 성별, 거주지역, 국적 등과 같이 해당 정보만으로는 직접적으로 특정 개인을 식별할 수 없지만, 다른 속성과 결합하여 특정 개인의 신원을 전부 또는 일부를 드러낼 수 있는 속성을 말한다.

〈 (예시) 속성의 분류 〉

속성	가명 · 익명처리 대상 정보
식별자	성명, 상세주소, 전화번호, 생체인식정보, 전자우편주소, 사회관계망서비스 주소, 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 「정보통신망법」 제23조의3에 따른 본인확인기관이 특정 개인을 고유하게 식별할 수 있도록 부여한 정보, 특정 개인을 고유하게 식별하거나 동일한 신용정보주체를 구분하기 위하여 부여된 정보, 국내거소신고번호, 계좌번호, 신용카드번호, 건강보험증번호, 기기식별자, 자동차번호 등
개인식별 가능정보	성별, 나이, 주소, 우편번호, 직업(직업명 혹은 직업코드), 사건발생일자(사망, 승인, 수술, 퇴원, 방문 등), 위치(우편번호, 건물명, 지역 등), 인종, 출생국, 모국어, 가시적 소수인종집단 지위(visible minority status), 결혼 여부, 학력, 범죄경력, 종교, 의료 진단명, 보험 가입정보(보험 종류, 가입건수, 가입채널, 가입일, 보장금액 등), 신용대출 정보(대출건수, 계약일, 대출액, 상환액, 연체율 등), 납입보험료, 추정소득, 추정주택가격, 보유차량 정보, 핵심고객 여부, 내부 신용등급, CB신용점수 등

다. 식별(identification)

단독으로 또는 두 개 이상의 속성을 결합하는 등의 방법으로 개인을 알아볼 수 있도록 처리하는 것을 말한다.

◎ 「**신용정보법**」 **제2조(정의) 13.** "처리"란 신용정보의 수집(조사를 포함한다. 이하 같다), 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 결합, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

라. 정보집합물

정보를 체계적으로 관리하거나 처리할 목적으로 일정한 규칙에 따라 구성되거나 배열된 둘 이상의 정보들을 말한다(신용정보법 제2조제15호 나목).

마. 결합키

결합의뢰기관이 정보집합물을 데이터전문기관에 제공하는 경우 하나의 정보집합물과 다른 정보집합물간에 둘 이상의 정보를 연계, 연동하기 위하여 사용되는 정보로, 해당 개인을 식별할 수 없으나 구별할 수 있는 정보를 말한다.

바. 가명처리

추가정보(예 : 가명정보와 기존 식별자를 연결하는 매핑테이블 등)를 사용하지 아니하고는 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리하는 것을 말하는데, 그 처리 결과가 ① 어떤 신용정보주체와 다른 신용정보주체가 구별되는 경우 ② 하나의 정보집합물에서나 서로 다른 둘 이상의 정보집합물 간에 어떤 신용정보주체에 관한 둘 이상의 정보가 연계되거나 연동되는 경우 ③ 위와 유사한 경우로서 대통령령으로 정한 경우의 어느 하나에 해당하는 경우로서 법령에 따라 그 추가정보를 분리하는 등 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리한 경우를 포함한다(신용정보법 제2호제15호).

사. 가명정보

가명처리한 개인신용정보를 말한다(신용정보법 제2조제16호).

아. 추가정보

특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 가명처리 하는데 사용된 정보로서 가명정보를 원래의 상태로 복원하는데 사용할 수 있는 값을 말한다.

※ (예시) 가명정보와 기존 식별자를 연결하는 매핑테이블, 가명정보 생성시 사용한 암호 알고리즘, 가명정보 생성시 사용한 솔트값 등

자.익명처리

데이터 값 삭제, 가명처리, 총계처리, 범주화 등의 방법으로 개인신용정보의 전부 또는 일부를 삭제하거나 대체함으로써 더 이상 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리하는 것을 말한다(신용정보법 제2조제17호).

차.익명정보

개인신용정보를 더 이상 특정 개인인 신용정보주체를 알아볼 수 없도록 익명처리한 정보를 말한다.

카. 결합 대상 정보집합물

결합의뢰기관이 결합을 위해 데이터전문기관에 제공하는 정보집합물을 말한다.

타. 결합정보

데이터전문기관을 통해 결합된 정보집합물을 말한다.

파. 연결키

결합의뢰기관이 결합정보를 이용하여 시계열 분석·연구 등을 수행할 수 있도록 데이터전문기관이 결합키를 대체하여 제공하는 값을 말한다.

3. 개인정보, 가명정보, 익명정보

「신용정보법」은 가명처리와 익명처리 개념을 도입하였다. 개인정보에서 가명정보, 익명정보로 갈수록 식별가능성이 낮아지게 된다. 개인정보, 가명정보 및 익명정보를 개념 및 활용 가능한 범위를 기준으로 구분하면 다음과 같다.

구분	개념	활용가능 범위
개인정보	특정 **개인에 관한 정보**, 개인을 **알아볼 수 있게 하는 정보**	**정보주체**로부터 **사전에 구체적인 동의를** 받은 범위 등의 내에서 활용 가능
가명정보	**추가정보**의 사용 없이는 **특정 개인을 알아볼 수 없게 조치**한 정보	다음 목적으로는 **동의 없이** 활용 가능 ❶ 통계작성(상업적 목적 포함) ❷ 연구(산업적 연구 포함) ❸ 공익적 기록보존 목적 등
익명정보	**더 이상 개인을 알아볼 수 없게 조치**한 정보	개인정보가 아니기 때문에 **제한 없이 자유롭게 활용**

※ 구체적인 개인정보, 가명정보, 익명정보의 예시는 아래 참조

[가명정보와 익명정보 예시]

■ **원본 정보집합물 정보**

〈 (예시) 원본 정보 〉

성명	전화번호	성별	생년월일	보험가입건수
신사임당	010-1234-5678	여	1974.10.1.	3
권율	02-2345-6789	남	1990.3.26.	2
유관순	010-3456-4321	여	1969.5.28.	1
이순신	010-4567-9876	남	1993.11.3.	2
선덕여왕	010-5678-9012	여	1971.1.2.	3
안중근	010-6789-0123	남	1988.7.16.	3
류성룡	010-7890-1234	남	1994.2.3.	2
이황	010-8901-2345	남	1982.6.28.	5
이이	010-9012-3456	남	1985.8.5.	2
…	…	…	…	…
식별자		개인식별가능정보		

❶ 가명정보

〈 (예시) 가명처리된 정보 〉

ID	~~성명~~	~~전화번호~~	성별	출생년도	보험 가입건수
9A00F1155584BA5DDFFC4B6DDD7940431737C612651267FBD4716FE93C46F6BA	~~신사임당~~	~~010-1234-5678~~	여	1974	3
C2E6376B9035D7067C8B68F25FA34592F210D72E59B8E3F018C941B391AB1D99	~~권율~~	~~02-2345-6789~~	남	1990	2
DACE2CCC9F459387EAE890D8534955003F78B2B474C997CF2D990573D4C3344F	~~유관순~~	~~010-3456-4321~~	여	1969	1
27B339D75FF1DCED2C29A866BA5D61555D4C2E2C708F121AFABF34E5777AE498	~~이순신~~	~~010-4567-9876~~	남	1993	2
6CE926B166980F9C5F05F0B19A443E3494943BDACF2A657DFA1B2CF37C17B839	~~선덕여왕~~	~~010-5678-9012~~	여	1971	3
05CF80408DCC19A18228A365BD2DBBD4328BC36DC832F6E7365E536164A92B5A	~~안중근~~	~~010-6789-0123~~	남	1988	3
11834268AF3110DB64360198755400A49AF1A60A0BFE624DCE108B9E1185FA6C	~~류성룡~~	~~010-7890-1234~~	남	1994	2
725F8676075F7C0C5E6655EE84FF0EA2BEFD57D7F6C338083A961C211AAE952D	~~이황~~	~~010-8901-2345~~	남	1982	5
380A314D13F03BB6DBBAA0EAC76E26C1ED3A19A7AA7466116286 1D021FDEED7E	~~이이~~	~~010-9012-3456~~	남	1985	2
…	…	…	…	…	…

- 성명, 전화번호, 성별, 생년월일을 조합하여 가명처리 기법 중 하나인 해시함수(SHA-256, 솔트값)를 적용
- 식별자(성명, 전화번호)는 삭제하고 개인식별가능정보(성별, 생년월일, 보험 가입건수)는 활용하되 개인 식별 가능성이 높은 성별, 생년월일 등은 일반화 처리* 가능

* 가명정보 이용자의 개인정보 보호수준과 가명정보의 재식별 가능성 등에 따라 가명처리 수준은 달라질 수 있음(위험도가 높을수록 가명처리 수준도 높아짐)

※ (예시) 원본정보(1974.9.23.) → 출생년도만 남김(1974년) → 연령대로 범주화(40대)

❷ 익명정보

〈 (예시) 익명처리된 정보 〉

~~성명~~	~~전화번호~~	성별	연령대	보험 가입건수	
~~권율~~	~~02-2345-6789~~	D	20대	2	동질집합 (k=3)
~~이순신~~	~~010-4567-9876~~	D	20대	2	
~~류성룡~~	010-7890-1234	D	20대	2	
~~안중근~~	~~010-6789-0123~~	D	30대	3	동질집합 (k=3)
~~이황~~	~~010-8901-2345~~	D	30대	5	
~~이이~~	~~010-9012-3456~~	D	30대	2	
~~신사임당~~	~~010-1234-5678~~	C	40대	3	동질집합 (k=3)
~~유관순~~	~~010-3456-4321~~	C	40대	1	
~~선덕여왕~~	~~010-5678-9012~~	C	40대	3	
		…	…	…	

- 식별자(성명, 전화번호)는 삭제
- 개인식별가능정보 중 다른 속성과 결합할 때 개인 식별 가능성이 높은 '성별'은 직접 알아볼 수 없도록 코드 형태로 변환(여성→C/남성→D)
- 개인식별가능정보 중 다른 속성과 결합할 때 개인 식별 가능성이 높은 '생년월일'은 k-익명성*을 충족하기 위해 삭제하고, 연령대로 범주화

  * k값은 익명정보 이용 목적, 환경 등에 따라 상이

  ※ 본 안내서 'Ⅲ. 2. 익명처리 방법'을 참고
- '보험 가입 건수'는 분석 대상이 되는 속성이고 다른 속성과 결합할 때 개인 식별 가능성이 낮다고 판단되어 변환하지 않음

4.금융분야 가명 · 익명처리 일반

가. 가명정보의 활용 범위

가명정보는 통계작성(상업적 목적을 포함), 연구(산업적 연구를 포함), 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우에는 개인인 신용정보주체의 동의 없이 가명정보를 활용할 수 있다(「신용정보법」 제32조제6항제9호의2). 이 경우 통계작성에는 시장조사 등 상업적 목적으로 수행하는 통계작성을 포함하며, 연구에는 대학, 연구소 등 연구기관 뿐 아니라 기업 등이 수행하는 산업적 연구를 포함한다. 다만, 특정 개인을 식별할 수 있는 형태의 통계작성, 연구, 공익적 기록 보존 등의 행위는 모두 허용되지 않는다.

• **(통계작성)** 집단적 현상이나 수집된 자료의 내용에 관한 수량적인 정보를 작성하는 행위

◎ **예시**

▶ 금융기관 소액대출 심사의 신용 보조지표로 활용하기 위하여 고객 · 지역별 신용카드 결제 데이터, 아파트 관리비, 부동산 시세 등에 대한 통계를 작성하는 경우

▶ 지자체 쓰레기 수거량을 예측하기 위하여 신용카드 결제건수 · 이용금액, 가맹점 업종 · 지역, 고객 거주 · 직장 지역, 거주 지역별 온 · 오프라인 구매물품, 배달음식 매출액 · 건수 등에 관한 통계를 작성하는 경우

• **(연구)** 기술 개발, 실증, 기초연구, 응용연구, 민간투자연구 등 과학적 방법을 적용하는 연구를 의미

– 자연과학적 연구뿐만 아니라 과학적 방법을 적용하는 역사적 연구, 공중보건 분야에서 공익을 위해 시행되는 연구 등은 물론, 새로운 기술 · 제품 · 서비스의 개발, 시장조사 등 산업적 목적의 연구도 포함

◎ **예시**

▶ 보험사기 자동 탐지시스템 개발을 위하여 과거 10년간의 보험사기 사례에 대한 보험금 청구금액, 청구시점과 방법, 유사청구 반복 여부 등을 분석하여 보험사기의 징후를 발견하기 위한 연구를 하는 경우

• **(공익적 기록보존)** 공공의 이익을 위하여 지속적으로 열람할 가치가 있는 기록정보를 보존하는 것을 의미

– 공공기관이 처리하는 경우에만 공익적 목적이 인정되는 것은 아니며, 민간기업, 단체 등이 일반적인 공익을 위하여 기록을 보존하는 경우도 공익적 기록 보존 목적이 인정됨

◎ **예시**

▶ 연구소가 현대사 연구 과정에서 수집한 개인정보 중에서 사료가치가 있는 인물정보를 기록하여 보관하는 경우

나. 익명정보의 활용 범위

익명정보는 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리한 것으로, 개인을 알아볼 수 없는 정보임을 전제(「신용정보법」제2조제17호)로, 별도의 제한 없이 사용할 수 있다.

다. 가명처리 관련 의무 및 처벌 규정

신용정보회사등은 가명처리에 사용한 추가정보를 기술적 · 관리적 · 물리적 보호조치를 통해 추가정보에 대한 접근을 통제하는 방법으로 분리하여 보관하거나 삭제하여야 하며(「신용정보법」 제40조의2제1항), 가명처리한 개인신용정보에 대하여 제3자의 불법적인 접근, 입력된 정보의 변경 · 훼손 및 파괴, 그 밖의 위험으로부터 가명정보를 보호하기 위하여 내부관리계획을 수립하고 접속기록을 보관하는 등 기술적 · 관리적 · 물리적 보안대책을 수립 · 시행하여야 한다(「신용정보법」 제40조의2제2항).

또한 신용정보회사등은 영리 또는 부정한 목적으로 특정 개인을 알아볼 수 있게 가명정보를 처리하여서는 아니 되며(「신용정보법」제42조의2제6항), 신용정보회사등이 영리 또는 부정한 목적으로 특정 개인을 알아볼 수 있게 가명정보를 처리한 경우, 금융위원회는 관련 매출액이 아닌 '전체 매출액'의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다(「신용정보법」제42조의2제1항 제1호의4).

그리고 영리 또는 부정한 목적으로 특정 개인을 알아볼 수 있게 가명정보를 처리한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처해질 수 있다(「신용정보법」제50조제2항 제7호의2).

※ 「신용정보법」 제40조의2 제1항 내지 제2항의 사항은 신용정보법 시행령 제34조의5제1항 내지 제3항에 정하고 있으며, 「신용정보업 감독규정」 제43조의7 및 [별표 8]에 금융위원회는 그 세부사항을 규정(본 안내서 'Ⅱ. 5. 가명정보 및 추가정보에 관한 보호조치 기준' 참고)

한편, 가명처리에 사용한 추가정보를 분리하여 보관하거나 삭제하지 아니한 자, 가명처리한 개인신용정보에 대하여 기술적 · 관리적 · 물리적 보안대책을 수립 · 시행하지 아니한 자, 가명정보를 이용하는 과정에서 특정 개인을 알아볼 수 있게 된 경우 즉시 그 가명정보를 회수하여 처리를 중지하거나 즉시 삭제하지 아니하는 자는 3천만원 이하의 과태료에 처해질 수 있다(「신용정보법」제52조제3항 제16호 내지 제18호).

라. 익명처리 적정성 평가

신용정보회사등은 개인신용정보에 대한 익명처리가 적정하게 이루어졌는지 여부에 대하여 금융위원회에 그 심사를 요청할 수 있다(「신용정보법」제40조의2제3항). 금융위원회가 위 요청에 따라 심사하여 적정하게 익명처리가 이루어졌다고 인정한 경우 더 이상 해당 개인인 신용정보주체를 알아볼 수 없는 정보로 추정한다(「신용정보법」 제40조의2제4항).

금융위원회는 「신용정보법」제40조의2제3항의 익명처리의 적정성 심사 및 「신용정보법」제40조의2제4항의 익명처리의 적정성 인정업무를 데이터전문기관에 위탁한다(「신용정보법 시행령」제37조제5항).

마. 가명 • 익명처리의 조치 기록 보존 의무

신용정보회사등은 개인신용정보를 가명처리한 경우에는 가명처리한 날짜, 가명처리한 정보의 항목, 가명처리한 사유와 근거를, 개인신용정보를 익명처리한 경우에는 익명처리한 날짜, 익명처리한 정보의 항목, 익명처리한 사유와 근거를 3년간 보존하여야 한다(「신용정보법」 제40조의2제8항).

위 보존의무를 위반하여 개인신용정보를 가명처리하거나 익명처리한 기록을 보존하지 아니한 자에게는 1천만원 이하의 과태료를 부과한다(「신용정보법」 제52조제5항 제11호의3).

데이터전문기관

「신용정보법」 제26조의4 및 「신용정보법 시행령」 제22조의4에 따라 정보집합물 결합과 익명처리에 대한 적정성 평가 업무와 정보집합물 결합과 가명 · 익명처리에 대한 조사 · 연구 · 표준화 등의 업무 수행

Ⅱ. 가명처리

Ⅱ. 가명처리

1. 개 요

식별자는 원칙적으로 삭제하여야 하며, 정보집합물 결합 등 데이터 이용목적 상 필요한 경우 안전한 방식으로 대체값을 생성하여 식별자를 대체하여야 한다.

개인식별가능정보는 금융분야에서 처리하는 개인신용정보 및 이용환경의 특성에 따라 개인식별가능정보 간의 조합, 외부에 공개된 정보와의 결합, 특이치(outlier)* 등으로 인하여 개인 식별 가능성이 높은 경우 일반화, 범주화 등의 추가적인 조치를 통해 재식별 위험을 낮춰야 한다. 또한 개별 속성에 대한 가명처리 수준은 가명처리 목적, 가명정보 이용환경과 가명정보 및 추가정보에 대한 보호조치 수준에 따라 달라질 수 있다. 예를 들어, 내부 연구목적으로 가명정보를 활용하려는 경우 생년월일 정보를 출생년도로 이미 처리했더라도, 동일한 가명정보를 제3자에게 제공하는 경우에는 가명처리 수준을 10세 단위의 연령으로 높일 수 있다. 개인식별가능정보는 개인 식별의 위험이 높지 않다면 원칙적으로 별도의 조치 없이 사용할 수 있다. 다만, 이용 상황에 따라 개인 식별 가능성이 높아진 경우에는 추가적인 조치를 통해 재식별 위험을 낮춰야 한다.

* 관측된 데이터의 범위에서 많이 벗어난 아주 작은 값이나 아주 큰 값

◎ **특이치 예시**

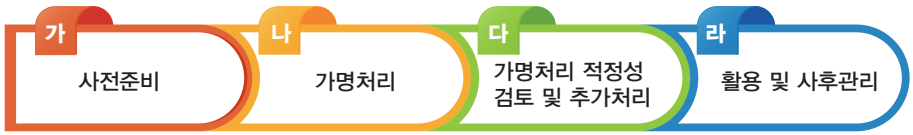
▶ 신용정보주체의 연령이 20세에서 75세 사이에 대부분 분포하는 데이터셋에서 특정 신용정보주체의 연령만 110세인 경우

▶ 신용정보주체의 대출금액이 5백만원에서 10억원 사이에 대부분 분포하는 데이터셋에서 특정 신용정보주체의 대출금액이 80억원인 경우

2. 가명처리 절차

신용정보회사등은 다음의 절차 예시 등을 참고하여 가명정보의 위험도를 검토하고 그에 따른 적절한 가명처리를 수행하여야 한다.

〈 (예시) 가명처리 단계별 절차 〉



가. 사전준비

가명처리 목적을 명확히 정의하여 그에 따른 가명처리 대상 데이터를 추출하고, 가명정보 처리 및 활용에 대한 내부 체계를 구축하여야 한다. 신용정보회사등이 가명정보를 제3자에게 제공할 경우, 사후 책임문제를 명확하게 하기 위하여 재식별 금지, 정보유출시 손해배상 등을 반영한 계약서를 작성할 필요가 있다.

- **(가명처리 목적 명확화)** 가명정보의 활용 목적은 「신용정보법」에서 허용하는 목적 내에서 최대한 구체화

  ※ 통계작성(상업적 목적 포함), 연구(산업적 연구 포함), 공익적 기록보존 목적 등

- **(처리대상 추출)** 가명처리 목적을 달성하기 위해 반드시 필요한 최소한의 항목으로 가명처리 대상 정보집합물을 추출

- **(가명정보 처리 및 활용 체계 구축)** 가명정보 활용에 대한 관리방안을 수립하고 가명정보 및 추가정보에 대한 접근관리 체계를 구축*

  * 가명정보 및 추가정보에 대한 접근통제 등 관리방안 수립 등('Ⅱ. 4. 가명처리에 관한 행위규칙' 참고)

나. 가명처리

가명처리 및 가명정보 이용 환경, 가명처리 대상 데이터의 특성 등을 고려하여 위험도를 측정하고 가명처리 수준을 결정한 후 가명처리를 수행한다.

• **(위험도 측정)** 가명처리 목적, 처리 · 이용 환경 및 가명처리 대상 데이터의 특성 등에 따른 위험도 분석

〈 (예시) 위험도 측정시 고려사항 〉

고려사항	세부 내용
가명처리 목적	통계작성(상업적 목적 포함), 연구(산업적 연구 포함), 공익적 기록보존 목적 여부 등 범위내에서 세부적인 목적
가명정보 활용 주체	내부 활용/내부 결합/외부 제공/외부 결합/외부 공개 여부 등
가명처리 · 이용 환경	처리 환경 및 이용(분석) 환경의 내부통제 수준, 재식별 의도 또는 능력 등 ※ 'Ⅱ. 3. 라. 가명정보의 재식별 위험도 측정시 고려사항' 참고
가명처리 대상 데이터의 특징 분석	가명처리 대상 데이터의 특성 분석 데이터 속성(칼럼)을 식별자, 개인식별가능정보 등으로 분류 ※ 식별자, 개인식별가능정보 예시는 'Ⅰ. 2. 나. 속성' 참고

• **(가명처리 수준 결정)** 위험도를 고려하여 적절한 가명처리 방법 · 수준을 결정하고 가명정보 및 추가정보의 보유기간을 정의*

* 가명정보의 이용목적, 가명처리의 기술적 특성, 정보의 속성, 추가정보에 대한 기술적 · 관리적 · 물리적 보호조치 수준, 가명정보의 재식별시 신용정보주체에 미치는 영향, 가명정보의 재식별 가능성, 가명정보의 이용목적 및 그 목적 달성에 필요한 최소기간 등을 고려

• **(가명처리)** 식별자의 삭제 또는 대체*, 재식별 위험도가 높은 개인식별가능정보에 대한 가명처리** 등을 수행

* 대체값 생성시 랜덤값 생성, 해시값 생성, 암호화 등 안전한 방식 활용 필요('Ⅱ. 3. 나. 식별자의 대체값 생성 방법' 및 'Ⅱ. 3. 다. 속성별 가명처리 방법' 참고)

** 일반화, 범주화, 상 · 하단 코딩, 레코드 삭제 등의 기법 활용('부록 1. 가명 · 익명처리 기법' 참고)

다. 가명처리 적정성 검토 및 추가처리

앞의 '나 단계(가명처리)'에서 가명처리 수준이 적절히 정의되었고 이에 따라 가명처리가 제대로 되었는지 여부를 확인하고, 재식별 가능성 등을 검토하여 필요시 추가로 가명처리를 수행한다.

- **(적정성 검토)** 내부자 또는 필요시 외부 전문가를 활용하여 가명정보의 개인 식별 가능성(식별자 존재 여부, 가명처리 수준의 적절성 등)을 검토

> ◎ **예시**
>
> ▶ 연구 목적으로 가명처리한 데이터를 대상으로 내부 개인정보보호 책임자 및 외부의 법률 전문가 1명, 가명 · 익명처리 전문가 1명을 포함한 평가회의를 개최하여 가명처리의 적정성을 검토

※ 본 절차는 필수 사항은 아니며, 필요에 따라 신용정보회사등이 자체 절차를 수립하여 이행할 수 있음

라. 활용 및 사후관리

가명정보를 이용 · 제공 · 결합한 후 가명정보의 파기 등 가명정보 활용에 대한 행위규칙 등을 준수한다.

※ 'Ⅱ. 4. 가명처리에 관한 행위규칙' 및 'Ⅱ. 5. 가명정보 및 추가정보에 관한 보호조치 기준' 참고

〈 (예시) 가명처리 세부 절차 〉

단계	절차	내용
가. 사전 준비	사전 준비	• 가명처리 목적 정의 • 가명처리 대상 정보집합물 추출 • 가명정보 및 추가정보에 대한 접근통제 등 관리방안 수립 등
나. 가명 처리	위험도 측정	• 가명처리 목적, 처리 · 이용환경(내부통제 수준, 재식별 의도 및 능력 등), 이용 주체(내부 활용/내부 결합/외부 제공/외부 결합/외부 공개 여부) 등에 따른 위험도(Risk) 분석 • 가명처리 대상 정보집합물의 특성 분석 • 데이터 속성(칼럼)을 식별자, 개인식별가능정보 등으로 분류 ※ 식별자, 개인식별가능정보 예시는 'Ⅰ. 2. 나. 속성' 참고
	가명처리 수준 결정	• 가명처리 방법 및 수준 결정 • 가명정보 및 추가정보의 보유기간 정의 ※ 가명정보의 이용목적, 가명처리의 기술적 특성, 정보의 속성, 추가정보에 대한 기술적 · 관리적 · 물리적 보호조치 수준, 가명정보의 재식별시 신용정보주체에 미치는 영향, 가명정보의 재식별 가능성, 가명정보의 이용목적 및 그 목적 달성에 필요한 최소기간 등을 고려
	가명처리	• 식별자에 대하여 삭제 또는 대체 • 대체값 생성시 안전한 방식 활용 필요 : 랜덤값 생성, 해시값 생성, 암호화 등 ※ 대체값 생성 알고리즘, 매핑테이블, 암호키 등 추가정보는 삭제 또는 분리보관 • 이용 · 제공 상황에 따라 재식별 리스크가 높다고 판단되는 경우, 개인식별가능정보에 대한 추가적인 가명처리* * 일반화, 범주화, 상 · 하단 코딩, 레코드 삭제 등의 기법 활용(본 안내서 '부록 1. 가명 · 익명처리 기법' 참고)

단계	절차	내용
다. 적정성 검토	(필요시) 가명처리 적정성 검토	• 가명정보의 개인 식별 가능성 검토(식별자 존재 여부, 가명처리 수준의 적절성 등) • 내부자 검토 또는 (필요 시) 외부 전문가 활용 ※ 본 절차는 필수 사항은 아니며 필요에 따라 내부 절차를 수립하여 이행할 수 있음
라. 활용 및 사후관리	가명정보 이용 · 제공 · 결합 및 사후관리	• 통계작성, 연구, 공익적 기록보존 등의 목적으로는 신용정보주체의 동의 없이 가명정보 이용 또는 제공 가능 • 가명정보의 제3자 제공시 재식별 시도 금지, 책임 범위, 보호조치, 목적외 사용금지, 재제공 금지 등에 대한 사항을 계약 등을 통해 명시 필요 • 신용정보회사등의 경우 제3자와의 정보집합물 결합은 금융위원회가 지정한 데이터전문기관을 통해서만 가능 • 가명처리시 가명처리한 날짜, 정보의 항목, 사유와 근거를 기록하고 3년간 보존 • 「신용정보법」 제40조의2(가명처리 · 익명처리에 관한 행위규칙)에 따라 추가정보는 분리하여 보관하거나 삭제하고 가명정보를 안전하게 보호하기 위하여 내부관리계획을 수립하고 접속기록을 보관하는 등 기술적 · 관리적 · 물리적 보안대책을 수립 · 시행 • 가명정보를 이용하는 과정에서 특정 개인을 알아볼 수 있게 된 경우 즉시 그 가명정보를 회수하여 처리를 중지하고, 특정 개인을 알아볼 수 있게 된 정보는 즉시 삭제
	가명정보 삭제	• 가명처리 계획 수립시 정한 가명정보 보유 기간이 도래한 경우 삭제 조치 • 추가정보에 대해서도 반드시 필요하지 않은 경우 삭제 조치

3. 가명처리 방법

가. 가명처리 기법

1) 일반화, 범주화, 상 · 하단 코딩, 레코드 삭제 등 여러 가지 기법을 단독 또는 복합적으로 활용해야 한다.

2) 대체값 생성시 랜덤값 생성, 해시값 생성, 암호화 등 안전한 방식의 기법을 활용해야 한다.

3) 각각의 기법에는 이를 구현할 수 있는 다양한 세부기술이 있으며, 데이터 이용 목적과 기법별 장단점 등을 고려하야 적절한 기법 및 세부기술을 선택하고 활용해야 한다.

※ '부록 1. 가명 · 익명처리 기법' 참고

나. 식별자 조치방법

신용정보회사등은 가명처리할 때 정보집합물 내의 식별자는 삭제하거나 가명으로 대체하여야 한다. 금융분야에서 사용되는 주요 식별자의 예시는 아래와 같다. 아래 예시 외에도 데이터 특성 및 이용환경 등에 따라 특정 신용정보주체를 식별할 수 있는 정보가 존재한다면 식별자에 해당할 수 있다.

◎ 금융분야 식별자 예시

▶ 성명, 상세주소, 전화번호, 바이오인식정보(지문, 홍채, 안면인식 등), 전자우편주소, 사회관계망서비스 주소, 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 정보통신망법 제23조의3에 따른 본인확인기관이 특정 개인을 고유하게 식별할 수 있도록 부여한 정보(CI, DI), 특정 개인을 고유하게 식별하거나 동일한 신용정보주체를 구분하기 위하여 부여된 정보(회원번호, 고객번호, 아이디, 멤버십번호 등), 국내거소신고번호, 계좌번호, 신용카드번호, 건강보험증번호, 기기식별자(IMEI 등), 자동차번호, 그 밖에 특정 개인을 고유하게 식별할 수 있는 정보(사진, 영상 등)

[식별자의 대체값 생성 방법]

식별자의 대체값(이하'가명(pseudonym)')은 일반적으로 랜덤값 생성, 해시값 생성, 암호화 기법 등을 활용할 수 있으며, 그 외에 이와 동일한 수준의 안전성을 확보할 수 있는 다른 방식(토큰화 등)을 활용할 수 있다. 가명 생성시 사용된 추가정보(매핑테이블, 암호키, 암호 알고리즘 등)*는 분리하여 보관하거나 삭제하는 등 「신용정보법」 제40조의2(가명처리·익명처리에 관한 행위규칙)에 따라 안전하게 관리되어야 한다.

* 가명과 원본의 식별자를 연결하는 매핑테이블을 생성할 수 있으며, 이 경우 매핑테이블이 추가정보에 해당

1) 랜덤값 생성

랜덤값 생성은 식별자에 대하여 독립적인 가명을 생성하는 방법으로, 랜덤값을 생성하여 원본값을 대체하는 방식을 말한다. 랜덤값 생성시 안전한 난수발생기(Random Number Generator, RNG)를 사용하여야 하며 난수 생성규칙이 노출되거나 중복이 발생하지 않도록 주의하여야 한다.

〈 (예시) 랜덤값 생성을 통한 가명처리 예시 〉

원본정보

고객번호	이름	연락처	이메일	대출액	...
1000000001	홍길동	010-1111-11111	abc@aaa.com	2,000,000	...
1000000002	임꺽정	010-2222-22222	yyy@aaa.com	45,000,000	...
1000000003	성춘향	010-3333-3333	zzz@bbb.com	500,000,000	...
...	....	...	...	...	...

추가 정보 (매핑 테이블)

※ 분리 보관 또는 삭제

고객번호	가명고객번호 ※랜덤값
1000000001	456234423484840237383834223241237477202
1000000002	923189131023848329037602872236512306521
1000000003	023783473246741136685229943101073527129
...	...

가명정보

가명고객번호	대출액	...
456234423484840237383834223241237477202	2,000,000	...
923189131023848329037602872236512306521	45,000,000	...
023783473246741136685229943101073527129	500,000,000	...
...	...	...

◎ **추가정보 예시**

▶ 가명(랜덤값)과 원본 식별자를 연결하는 매핑 테이블을 생성할 수 있으며, 이 경우 매핑 테이블이 추가정보에 해당

2) 해시값 생성

해시값 생성은 암호기술을 사용하여 식별속성으로부터 파생된 가명을 생성하는 방식으로서 단방향(one-way) 및 충돌 방지(collision-resistance) 특성을 가진 해시함수를 사용하여 단일 식별자 또는 다수 식별자들을 해시값으로 대체하는 방식을 말한다.

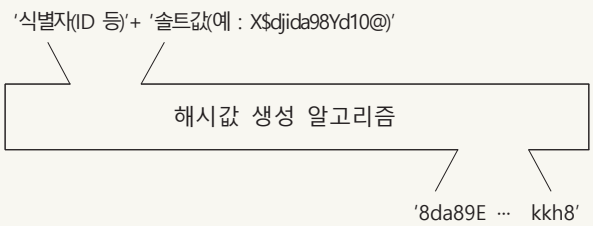
해시값에 대한 무작위 대입 공격*, 레인보우 테이블 공격** 등에 안전할 수 있도록 솔트값 또는 키값(key)을 추가하여 해시하여야 한다.

* 무작위 대입 공격(brute force attack) : 경우의 수를 무작위로 대입하여 원본값을 알아내는 공격

** 레인보우 테이블 공격(rainbow table attack) : 해시 함수를 사용하여 변환가능한 해시값을 미리 저장해 놓은 표를 통해 원본값을 알아내는 공격

해시값 생성시 사용되는 솔트값 또는 키값은 쉽게 유추할 수 없도록 복잡하게 구성하여야 하며 비인가자에게 노출되지 않도록 안전하게 관리하여야 한다.

〈 (예시) 해시 생성 예시 〉



식별자에 단순히 솔트값 또는 키값만 추가하여 해시를 생성하기 보다는 자체적으로 해시값 생성 규칙을 마련하여 해시값의 안전성을 높일 것을 권고한다.

해시값을 생성할 때 사용하는 해시 알고리즘은 SHA-2 이상의 안전성이 검증된 해시 알고리즘을 사용하여야 한다.

종류		출력값 길이(비트)	보안강도(비트)	참조 규격
SHA-2	224	224	112	NIST FIPS 180-4
	256	256	128	
	386	384	192	
	512	512	256	
SHA-3	224	224	112	NIST FIPS 202
	256	256	128	
	386	384	192	
	512	512	256	

〈 대표적인 권고 해시 알고리즘 〉

※ 출처 : 「금융부문 암호기술 활용가이드」(금융보안원, 2019.1.)

◎ **추가정보 예시**

▶ 필요시 가명(해시값)과 원본 식별자와의 매핑테이블을 생성 · 보관할 수 있으며 이때 사용한 솔트값 또는 키값, 해시값 생성규칙, 매핑 테이블 등이 추가정보에 해당

3) 암호화

가명 생성시 식별자를 암호화하는 방식을 사용할 수 있다. 이 때, SEED, AES, ARIA 등 안전한 암호 알고리즘 사용하여야 한다. 특히, 암호 알고리즘은 컴퓨팅 파워 증가, 기술의 발전 등에 따라 안전성에 변화가 발생할 수 있으므로 가명 생성 시점에 안전하다고 평가받는 암호 알고리즘을 확인하여 적용하여야 한다.

〈 대표적인 대칭키 블록암호 알고리즘 〉

종류	입출력 길이 (비트)	출력값 길이 (비트)	보안강도 (비트)	참조 규격
SEED	128	128	128	TTA TTAS.KO-12.0004/R1
AES	128	128	128	NIST FIPS 197
		192	192	
		192	192	

※ 출처 : 「금융부문 암호기술 활용가이드」(금융보안원, 2019.1.)

암호화에 사용된 키가 유출될 경우 유출된 키를 통해 암호문을 복호화 할 수 있으므로, 암호키 생성 · 배포 · 사용 · 정지 · 갱신 · 폐기 등의 암호키 관리절차 수립, 암호키의 분리 보관, 암호키에 대한 접근통제 조치 등 안전한 암호키 관리방안이 수립 · 이행되어야 한다.

◎ **추가정보 예시**

▶ 암호화 방식에서는 암호키, 암호 알고리즘 등이 추가정보에 해당

다. 개인식별가능정보 조치방법

개인식별가능정보 중 다른 정보와 결합할 경우 개인을 식별할 가능성이 높은 경우, 이용 · 제공 목적상 반드시 필요하지 않은 개인식별가능정보는 삭제하고 나머지 개인식별가능정보에 대해서는 적절한 수준의 추가 조치를 적용해야 한다. 금융분야에서 사용되는 주요 개인식별가능정보 및 조치사항 예시는 다음의 표와 같다.

〈 (예시) 금융분야 주요 개인식별가능정보 및 조치사항 〉

No	개인식별 가능정보	조치 사항 예시	비고
1	성별	• 이용 목적상 필요하다면 별도 조치 없이 사용가능하나 성별을 구분할 필요가 없는 경우 A, B 등으로 대체	일반화 등
2	나이	• 필요시 상황에 따라 5세, 10세 간격 등으로 범주화 • 특정 나이 이상 또는 이하의 경우 단일 범주로 집계(상 · 하단 코딩)	범주화, 상 · 하단 코딩 등
3	주소	• 세부주소의 경우 식별자에 해당하므로, 필요시 시 · 군 · 구 단위 등으로 범주화 • 특히 도서산간 등 일부 지역의 경우 읍 · 면 · 동 단위의 거주자가 매우 적을 수 있으므로 필요시 범주화 등 조치 필요 • 우편번호에 대해서도 동일한 기준 적용	범주화 등
4	직업	• 국회의원, 연예인, 운동선수 등 일부 직업의 경우 개인 식별 가능성이 높아지므로, 필요시 직업 분류에 명시적 으로 드러나지 않도록 조치	일반화, 범주화 등
5	국적	• 특정 집단 내에서 대다수가 동일 국적자인 경우, 그 외 국적자에 대한 개인 식별 가능성이 높아지므로 필요시 범주화 등 조치 필요	범주화 등
6	기념일	• 결혼기념일 등 일부 기념일의 경우 개인 식별 가능성이 높아지므로 필요시 범주화 등 조치	범주화 등
7	기혼여부	• 이용 목적상 필요하다면 별도 조치 없이 사용가능하나 기혼여부를 구분할 필요가 없는 경우 A, B 등으로 대체	일반화 등
8	거래지점	• 거래지점의 경우 거래자의 주요 활동지를 한정지을 수 있으므로 필요시 범주화 등 조치 필요 • 필요시 거래지점명/거래지점코드 대신 거래지점이 위치한 구 단위, 동 단위 주소 등으로 대체	범주화 등
9	기타	• 데이터 특성 상 다른 정보와 결합하여 개인을 식별할 가능성이 높은 속성이 존재한다면 개인 식별 가능성이 높은 개인식별가능정보로 지정 • 개인식별가능정보가 데이터 특성, 이용 상황, 제3자 제공 여부 등에 따라 재식별 위험이 높다고 판단되는 경우 추가 조치	일반화, 범주화, 잡음추가, 삭제, 상 · 하단 코딩 등

위의 예시에도 불구하고 데이터 특성 및 이용환경 등에 따라 추가 조치 필요 여부, 조치 방법 및 수준 등이 상이할 수 있으므로, 재식별 위험에 근거하여 적절한 조치를 취하여야 한다. 특히, 정보집합물을 외부에 제공하거나 결합하는 경우에는 재식별 위험이 높아질 수 있으므로 추가적인 조치를 고려할 필요가 있다.

라. 가명정보의 재식별 위험도 측정시 고려사항

가명정보의 재식별 위험도는 가명처리 수준을 결정하기 위한 주요한 요소이다. 가명정보 보호수준이 높은 이용기관에는 낮은 수준으로 가명처리 된 가명정보를 제공하여 활용성을 높이고, 보호수준이 낮은 이용기관에는 높은 수준으로 가명처리된 가명정보를 제공하여 개인신용정보가 재식별 될 수 있는 가능성을 줄여야 한다.

신용정보회사등이 이용기관의 가명정보 보호수준을 판단하기 위해서는 해당 이용기관의 재식별 의도와 능력, 가명정보 보호능력, 업무수행 신뢰도 등 다양한 측면에서 평가가 필요하며 이를 종합적으로 고려하여 가명처리 수준을 결정해야 한다.

1) 재식별 의도 및 능력 분석

가명정보 이용기관의 재식별 의도 및 능력에 대해 검토하고, 재식별 의도와 능력이 높게 평가될 경우 가명처리 수준을 높일 필요가 있다.

- **(재식별 의도)** 가명정보 이용자가 가명정보를 재식별하여 경제적 · 비경제적 이득을 취할 수 있거나, 목적에 부합하지 않는 범위로 가명정보를 활용할 여지가 있는지 등을 검토
- **(재식별 능력)** 가명정보 이용자가 재식별을 시도할 수 있는 전문지식이나 가명정보와 연계 가능한 데이터를 보유하고 있는지 등을 검토

2) 가명정보 보호수준 및 신뢰도 분석

가명정보도 개인신용정보로 볼 수 있으므로, 가명정보 이용기관의 가명정보 보호수준 및 업무수행 신뢰도에 대해 검토하고, 가명정보 보호능력과 업무수행 신뢰도가 낮게 평가될 경우 가명처리 수준을 높일 필요가 있다.

- **(가명정보 보호수준)** 가명정보 이용기관이 가명정보를 보호하기 위한 가명정보 관리계획을 수립 · 운영하고 기술적 · 관리적 · 물리적 보호조치를 마련하였는지, 개인정보 보호 관련 인증 유무 등을 검토
  ※ 「신용정보업 감독규정」 [별표 8] 가명정보에 관한 보호조치 기준 외에도, 동 규정의 [별표 3] 기술적 · 관리적 · 물리적 보안대책 마련 기준, 「개인정보보호법」 및 동 법률에 따른 「개인정보의 안전성 확보조치 기준」 등 관계 법령의 개인(신용)정보 보호를 위한 조치 기준을 준수하는지 여부에 대하여 판단
- **(업무수행 신뢰도)** 가명정보를 활용하면서 위법을 저지른 적은 없는지, 가명정보를 다른 기관에게 무단으로 제공할 가능성은 없는지 등을 검토

3) 분석 결과 해석

재식별 의도나 능력이 높다고 해서 무조건적으로 가명처리 수준을 높일 필요는 없다. 예를 들어 재식별 능력이 높다고 하더라도 가명정보 보호능력과 업무수행 신뢰도가 매우 높다면 가명처리 수준을 낮출 수 있을 것이다.

반대로 가명정보 보호능력과 업무수행 신뢰도가 높다고 해서 반드시 가명처리 수준을 낮춰서는 안 된다. 높은 보호능력을 가지고 있더라도 재식별 의도가 높아 보이는 등의 경우 가명처리 수준을 높여야 할 것이다.

[가명정보 이용환경에 따른 가명처리 예시]

▷ **처리 대상**

A 신용평가사가 보유한 개인사업자의 지방세 체납액, 대출잔액 등 신용정보

ID	성명	업종코드	생년월일	자가보유 여부	자가 예상시세	자택 주소	지방세 체납액 (만원)	대출 실행일	대출 잔액(원)
2345	홍길동	123456	1952.2.9.	보유	15.5억원	서울시 강남구 역삼동332-1	1,352	2005 10.10.	555,057,200
…	…	…	…			…	…		

▷ **가명정보 이용 환경 및 목적**

(사례 ①)

– (환경) A 신용평가사 자체적으로 내부 활용

– (목적) 지역별 개인사업자의 대출현황과 상환능력을 분석하여 내부 기획중인 신사업 타당성 판단

(사례 ②)

– (환경) B 신용카드사에 외부 제공

– (목적) 개인사업자 맞춤 대출심사전략을 마련

(사례 ③)

– (환경) C 대학연구실에 외부 제공

– (목적) C 대학이 위치한 특정 지역(대구광역시) 개인사업자의 대출현황과 상환능력을 분석하여 해당 지역 경제 현황 연구

① 가명정보의 위험성 검토

최소화 원칙

가명정보 이용 목적에 필요한 최소한의 항목을 선정하고 가명처리 수준을 높게 유지함으로써 재식별 위험성을 최소화

- 「ID」, 「**성명**」과 같은 식별자는 재식별이 불가능하도록 삭제처리 원칙
- 「**자택 주소**」는 개인이 식별되므로 그대로 활용할 경우 개인이 식별될 가능성이 매우 높아짐, 또한 C 대학 연구실의 이용 목적상 특정 지역(대구광역시)만 한정하여 추출
- 「**대출실행일자**」는 B 신용카드사 및 C 대학 연구실의 분석목적상 구체적일 필요는 없음
- 「**지방세 체납액**」, 「**대출잔액**」은 특이치가 있을 경우 개인이 식별될 가능성이 있음

② 가명정보 이용 환경에 따른 위험성 검토

사례 ①	A 신용평가사 자체적으로 내부 활용하는 경우	위험도	하
가명정보 내부관리계획에 따라 엄격한 기술적 · 관리적 · 물리적 보호조치를 적용하고 있으며 A 신용평가회사의 내부통제 하에 안전하게 활용 가능			

- 자체 보유 개인신용정보를 가명처리하여 분석하고자 하는 상황으로, 가명정보를 생성한 회사의 내부에서 가명정보가 활용되고 있어 가명정보를 불법적으로 재식별할 의도가 낮음

사례 ②	B 신용카드사에 외부 제공하는 경우	위험도	중
B 신용카드사는 A 신용평가회사와 마찬가지로 가명정보 내부관리계획에 따라 금융분야에서 요구하는 엄격한 기술적 · 관리적 · 물리적 보호조치를 적용하고 있으나, 외부제공에 따른 위험성이 존재하여 양사간 업무 협약서를 체결함으로써 비교적 안전하게 활용이 가능			

- 가명정보를 생성한 A 신용평가사 외부로 반출되어 활용되지만, B 신용카드사의 자체 내부관리계획과 양사간 협약서 등 다양한 측면을 고려하여 볼 때 가명정보를 불법적으로 재식별할 의도가 상대적으로 낮음

사례 ③	C 대학연구실에 외부 제공하는 경우	위험도	상
C 대학은 법령에서 요구하는 최소한의 기술적 · 관리적 보호조치를 적용하고 있으나 금융기관과 비교할 때 물리적 보호조치는 상대적으로 미흡			

- 가명정보를 생성한 A 신용평가사 외부로 반출되어 활용되고 C 대학 연구실의 보호수준이 높지 않은 것으로 확인되므로 개인신용정보가 재식별 되지 않도록 각별한 주의 필요

③ 가명처리 기준 결정

칼럼명	위험도에 따른 가명처리 수준		
	사례①	사례②	사례③
ID	식별자 삭제		
성명			
업종코드	–	마스킹 처리 (앞 네 자릿수 남김)	마스킹 처리 (앞 두 자릿수 남김)
생년월일	–	범주화(생년)	범주화(연령대)
자가 보유 여부	–	–	–
자가 예상 시세	–	–	삭제
자택 주소	범주화(동단위)		범주화(구단위) 및 해당지역 외 삭제
지방세 체납액	라운딩(십만원) 상단코딩(99.5%)	라운딩(백만원) 상단코딩(99.5%)	라운딩(백만원) 상단코딩(95%)
대출실행일	–	범주화(연월)	범주화(연월)
대출잔액	라운딩(천원) 상단코딩(99.5%)	라운딩(백만원) 상단코딩(99.5%)	라운딩(천만원) 상단코딩(99%)

④ 가명처리 결과

ID	성명	업종코드	생년월일	자가보유여부	자가 예상시세	자택 주소	지방세 체납액(만원)	대출 실행일	대출 잔액(원)
2345	홍길동	123456	1952.2.9.	보유	15.5억원	서울시 강남구 역삼동332-1	1,352	2005. 10.10.	555,057,200

가명처리

사례 1 A 신용평가사 자체적으로 내부 활용하는 경우

~~ID~~	~~성명~~	업종코드	생년월일	자가보유여부	자가 예상시세	자택 주소	지방세 체납액(만원)	대출 실행일	대출 잔액(원)
–	–	123456	1952.2.9.	보유	15.5억원	서울시 강남구역삼동	1,350	2005. 10.10.	555,057,000

사례 2 B 신용카드사에 외부 제공하는 경우

~~ID~~	~~성명~~	업종코드	생년월일	자가보유 여부	자가 예상시세	자택 주소	지방세 체납액 (만원)	대출 실행(월)	대출 잔액(원)
–	–	1234**	1952년	보유	15.5억원	서울시 강남구역삼동	1,350	2005. 10.10.	555,057,000

사례 3 C 대학연구실에 외부 제공하는 경우

~~ID~~	~~성명~~	업종코드	연령	자가보유 여부	~~자가 예상시세~~	자택 주소	지방세 체납액 (만원)	대출 실행(월)	대출 잔액(원)
–	–	~~12****~~	~~60대~~	~~보유~~	~~15.5억원~~	~~서울시 강남구~~	~~1,000~~	~~2005.10.~~	~~550,000,000~~
–	–	12***	30대	보유	3억원	대구시 달서구	587	2021.7.	330,000,000

4. 가명처리에 관한 행위규칙

※ 「신용정보법」 제40조의2(가명처리 · 익명처리에 관한 행위규칙), 「신용정보업감독규정」[별표 8] 가명정보에 관한 보호조치 기준(본 안내서 'Ⅱ. 5. 가명정보 및 추가정보에 관한 보호조치 기준' 참조) 등 참고

가. 추가정보의 분리 보관 또는 삭제

신용정보회사등은 가명처리에 사용한 추가정보를 분리하여 보관하거나 삭제하여야 한다. 이 때 금융위원회가 정하여 고시하는 기술적·관리적·물리적 보호조치를 통해 추가정보에 접근하는 것을 통제하는 방법을 준수하여야 한다.

나. 기술적 · 관리적 · 물리적 보안대책 수립 · 시행

신용정보회사등은 가명처리한 개인신용정보에 대하여 제3자의 불법적인 접근, 입력된 정보의 변경 · 훼손 및 파괴, 그 밖의 위험으로부터 가명정보를 보호하기 위하여 내부관리계획을 수립하고 접속기록을 보관하는 등 기술적 · 관리적 · 물리적 보안대책을 수립 · 시행하여야 하며, 다음 사항을 포함하여야 한다.

1) 가명처리한 개인신용정보에 제3자가 불법적으로 접근하는 것을 차단하기 위한 침입차단시스템 등 접근통제장치의 설치 · 운영에 관한 사항
2) 가명처리한 개인신용정보의 변경 · 훼손 및 파괴를 방지하기 위한 사항
3) 가명처리한 개인신용정보 취급 · 조회 권한을 직급별 · 업무별로 차등 부여하는 데에 관한 사항 및 가명처리한 개인신용정보 접근기록의 주기적인 점검에 관한 사항
4) 가명처리전 개인신용정보와 가명처리한 개인신용정보의 분리에 관한 사항
5) 가명정보를 통계작성, 연구, 공익적 기록보존 등의 목적으로 이용 · 제공할 경우 해당 목적 외 활용 방지에 관한 사항
6) 그 밖에 가명처리한 개인신용정보의 안전성 확보를 위하여 금융위원회가 정하여 고시하는 사항

다. 가명처리의 제한

신용정보회사등은 영리 또는 부정한 목적으로 특정 개인을 알아볼 수 있게 가명정보를 처리하여서는 아니 된다.

라. 재식별시 조치

신용정보회사등은 가명정보를 이용하는 과정에서 특정 개인을 알아볼 수 있게 된 경우 즉시 그 가명정보를 회수하여 처리를 중지하고, 특정 개인을 알아볼 수 있게 된 정보는 즉시 삭제하여야 한다.

신용정보회사등은 가명정보 재식별 이력이 있을 경우 신용정보관리 · 보호인에게 보고하고 기록 · 관리할 수 있도록 하여야 한다.

마. 가명처리 기록의 보존

신용정보회사등은 개인신용정보를 가명처리 한 경우 다음의 항목을 포함하여 그 조치 기록을 3년간 보존하여야 한다.

1) 가명처리한 날짜
2) 가명처리한 정보의 항목
3) 가명처리한 사유와 근거

〈 (예시) 가명처리 기록 〉

날짜	가명처리 근거	정보항목	가명처리 사유	가명처리 방법
2020. 9. 1.	① 가명처리 목적 연령대별 신용등급에 따른 연체율 연구 ② 관련 문서 첨부 (연구 계획(안) 등) ③ 근거 규정 「신용정보법」 제32조제6항 제9호의2 등	고객ID	식별자	삭제
		이름	식별자	이름, 휴대폰번호를 조합하여 해시함수 (SHA-256, 솔트값 적용)로 ID생성 후 삭제
		휴대폰 번호	식별자	
		나이	개인식별가능정보(재식별 가능성이 있고 연구목적상 구체적인 나이는 불필요)	연령대로 범주화
		대출 금액	개인식별가능정보(연구목적상 구체적인 수치는 불필요)	만원 단위로 반올림
		연체 기록	개인식별가능정보(구체적인 수치는 재식별 우려가 있음)	연체여부(Y/N)만 표기
		신용 등급	개인식별가능정보(신용등급은 이미 범주화된 등급이어서 재식별 우려가 거의 없음)	별도 조치 없음
		…	…	…
2020. 11. 3.	① 가명처리 목적 보험가입자 특성에 대한 동연구(X사의 데이터와 결합 후 분석) ② 관련 문서 첨부 (양사간 계약서, 공동연구 계획(안) 등) ③ 근거 규정 「신용정보법」 제17조의2, 제32조제6항 제9호의2, 동법 시행령 제14조의2 등	고객ID	식별자	삭제
		이름	식별자	이름, 휴대폰번호를 조합하여 해시함수 (SHA-256, 솔트값 적용)로 ID생성 후 삭제
		휴대폰 번호	식별자	
		거래 지점	개인식별가능정보(구체적인 지점 정보는 재식별 우려가 있음)	구 단위로 범주화
		보험 가입 건수	개인식별가능정보(구체적인 가입건수 수치는 재식별 우려가 낮음)	특이치만 삭제하고 별도 조치 없이 활용
		약관대출 금액	개인식별가능정보(연구목적 상 구체적인 수치는 불필요)	십만원 단위로 반올림
		…	…	…

바. 가명처리 관련 사항의 공개

가명정보는 통계작성, 연구, 공익적 기록보존 제한된 목적 내에서만 활용 가능한 특수한 형태의 개인신용정보이다. 따라서 가명정보를 처리하는 기관은 가명처리 관련 사항을 「신용정보법」, 「개인정보 보호법」 등과 같은 법률에 따라 공개하여야 한다.

신용정보회사, 신용정보집중기관 및 「신용정보법」시행령 제27조에서 정하는 신용정보제공 · 이용자는 가명정보 활용과 관련된 사항을 신용정보활용체제에 포함하여 공시하여야 한다 (「신용정보법」 제31조).

〈 (예시) 가명정보 처리 관련 신용정보활용체제에 포함될 사항 〉

1. 개인신용정보의 가명처리 관련 사항을 포함된 개인신용정보 보호 및 관리에 관한 기본계획
2. 처리하는 가명정보의 종류 및 이용 목적
3. 가명정보를 제3자에게 제공하는 경우 제공하는 가명정보의 종류, 제공 대상, 제공받는 자의 이용 목적
4. 가명정보의 보유 또는 이용 기간, 가명정보 파기의 절차 및 방법
5. 가명정보 처리의 위탁이 있는 경우 그 업무의 내용 및 수탁자
6. 처리하는 가명정보의 항목

◎ 「신용정보법」 제31조(신용정보활용체제의 공시)

① 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공 · 이용자는 다음 각 호의 사항을 대통령령으로 정하는 바에 따라 공시하여야 한다.

1. 개인신용정보 보호 및 관리에 관한 기본계획(총자산, 종업원 수 등을 고려하여 대통령령으로 정하는 자로 한정한다)
2. 관리하는 신용정보의 종류 및 이용 목적
3. 신용정보를 제공받는 자

4. 신용정보주체의 권리의 종류 및 행사 방법
5. 신용평가에 반영되는 신용정보의 종류, 반영비중 및 반영기간(개인신용평가회사, 개인사업자신용평가회사 및 기업신용등급제공업무 · 기술신용평가업무를 하는 기업신용조회회사로 한정한다)
6. 「개인정보 보호법」 제30조제1항제6호 및 제7호의 사항
7. 그 밖에 신용정보의 처리에 관한 사항으로서 대통령령으로 정하는 사항

◎ 「신용정보법 시행령」

제27조(신용정보활용체제의 공시) ① 법 제31조에서 "대통령령으로 정하는 신용정보제공 · 이용자"란 제5조제1항제1호부터 제21호까지 및 제21조제2항제1호부터 제21호까지의 규정의 어느 하나에 해당하는 기관을 말한다.

② 신용정보회사, 신용정보집중기관 및 제1항에 해당하는 자는 법 제31조에 따라 다음 각 호의 사항을 공시하여야 한다.

1. 관리하는 신용정보의 종류 및 이용 목적
2. 신용정보를 제3자에게 제공하는 경우 제공하는 신용정보의 종류, 제공 대상, 제공받는 자의 이용 목적(제1항에 해당하는 자로 한정한다)
3. 신용정보의 보유 기간 및 이용 기간이 있는 경우 해당 기간, 신용정보 파기의 절차 및 방법(제1항에 해당하는 자로 한정한다)
4. 법 제17조에 따라 신용정보의 처리를 위탁하는 경우 그 업무의 내용 및 수탁자
5. 신용정보주체의 권리와 그 행사방법
6. 법 제20조제3항에 따른 신용정보관리 · 보호인 또는 신용정보 관리 · 보호 관련 고충을 처리하는 사람의 성명, 부서 및 연락처
7. 신용등급 산정에 반영되는 신용정보의 종류, 반영비중 및 반영기간 (신용조회회사만 해당한다)

또한 개인정보처리자는 가명정보의 처리와 관련된 사항을 포함하여 개인정보처리방침을 작성 후 공개하여야 한다(「개인정보 보호법」 제30조).

◎ 「개인정보 보호법」 제30조(개인정보 처리방침의 수립 및 공개)

① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 "개인정보 처리방침"이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다.

1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)

3의2. 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)

4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
5. 정보주체와 법정대리인의 권리 · 의무 및 그 행사방법에 관한 사항
6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치 · 운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항

사. 가명정보에 대한 적용 예외

가명처리된 개인신용정보도 「신용정보법」상의 개인신용정보에 해당하나 동법은 개인신용정보에 적용되는 규정 중 보유기간, 개인신용정보 제공·활용에 대한 동의 등 일부에 대해서는 적용 예외를 두는 등 달리 정하고 있다.

◎「신용정보법」

제20조의2(개인신용정보의 보유기간 등) ②「개인정보 보호법」제21조제1항에도 불구하고 신용정보제공 · 이용자는 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 신용정보주체의 개인신용정보를 관리대상에서 삭제하여야 한다. 다만, 다음 각 호의 경우에는 그러하지 아니하다. 2의2. 가명정보를 이용하는 경우로서 그 이용 목적, 가명처리의 기술적 특성, 정보의 속성 등을 고려하여 대통령령으로 정하는 기간 동안 보존하는 경우

제40조의3(가명정보에 대한 적용 제외) 가명정보에 관하여는 제32조제7항, 제33조의2, 제35조, 제35조의2, 제35조의3, 제36조, 제36조의2, 제37조, 제38조, 제38조의2, 제38조의3, 제39조 및 제39조의2부터 제39조의4까지의 규정을 적용하지 아니한다.

제32조(개인신용정보의 제공 · 활용에 대한 동의)
제33조의2(개인신용정보의 전송요구)
제35조(신용정보 이용 및 제공사실의 조회)
제35조의2(개인신용평점 하락 가능성 등에 대한 설명의무)
제35조의3(신용정보제공 · 이용자의 사전통지)
제36조(상거래 거절 근거 신용정보의 고지 등)
제36조의2(자동화평가 결과에 대한 설명 및 이의제기 등)
제37조(개인신용정보 제공 동의 철회권 등)
제38조(신용정보의 열람 및 정정청구 등)
제38조의2(신용조회사실의 통지 요청)
제38조의3(개인신용정보의 삭제 요구)
제39조(무료 열람권)
제39조의2(채권자변동정보의 열람 등)
제39조의3(신용정보주체의 권리행사 방법 및 절차)
제39조의4(개인신용정보 누설통지 등)

5. 가명정보 및 추가정보에 관한 보호조치 기준

※ 「신용정보업감독규정」 [별표 8] 가명정보에 관한 보호조치 기준(제43조의7 관련)

가. 기술적 · 물리적 보호조치

1) 추가정보에 대한 보호조치

가) 신용정보회사등은 추가정보를 삭제하지 아니하고 보존하여야 하는 경우 추가정보를 가명정보와 분리된 저장소*에 암호화하여 저장하여야 한다.

※ 반드시 추가정보를 보존하여야 하는 경우를 제외하고는 추가정보를 삭제할 것을 권고

* 논리적 · 물리적 분리방법 모두 가능하나, 테이블을 분리하는 방법은 허용되지 않음

나) 신용정보회사등은 원칙적으로 가명정보를 취급하는 직원이 추가정보에 접근할 수 있는 권한을 부여하지 않아야 하며, 추가정보 접근이 불가피한 경우 관리책임자의 사전 승인을 받아 일시적으로 부여하고 관련 기록을 보관하는 등 적절한 통제시스템을 갖추어야 한다.

다) 신용정보회사등은 위 '나)'에 따른 기록 보관시 접근자의 신원, 관리책임자의 신원, 접근일시, 대상정보, 조회가 불가피한 사유, 용도 등의 기록을 3년간 보관하여야 한다.

라) 신용정보회사등은 추가정보가 가명정보를 재식별하는 데 사용되는 등 부정한 목적으로 사용되지 않도록 월 1회 이상 주기적으로 점검하여야 한다.

2) 가명정보에 대한 보호조치

가) 신용정보회사등은 가명처리전 개인신용정보와 가명처리한 개인신용정보를 분리하여 저장하여야 한다.

나) 신용정보회사등은 가명정보를 취급하는 담당자를 별도로 지정 · 관리하고 가명처리전 개인신용정보를 취급하는 담당자와 접근권한을 구분하여 운영하여야 한다.

다) 신용정보회사등은 원칙적으로 가명정보를 취급하는 직원이 가명처리전 개인신용정보에 접근할 수 있는 권한을 부여하지 않아야 하며, 원본정보 접근이 불가피한 경우 관리책임자의 사전 승인을 득하여 일시적으로 부여하고, 관련 기록을 보관하는 등 적절한 통제시스템을 갖추어야 한다.

라) 신용정보회사등은 위 '다)'에 따른 기록 보관시 접근자의 신원, 관리책임자의 신원, 접근일시, 대상정보, 접근이 불가피한 사유, 용도 등의 기록을 3년 이상 보관하여야 한다.

마) 신용정보회사등은 가명정보 처리 시 가명정보의 구체적인 처리 목적, 처리 방법, 처리 일시를 기록하여 가명정보가 파기된 이후 3년 이상 보관하고, 처리 기록에 대해 월 1회 이상 주기적으로 확인 · 감독하여야 한다.

바) 신용정보회사등은 가명정보 오·남용에 대한 자체 제재기준을 마련하여야 한다.

나. 관리적 보호조치

1) 신용정보회사등은 가명처리한 개인신용정보에 대하여 제3자의 불법적인 접근, 입력된 정보의 변경 · 훼손 및 파괴, 그 밖의 위험으로부터 가명정보를 보호하기 위해 다음 각 호의 사항을 포함하는 별도 내부관리계획을 수립 · 시행하여야 한다.

가) 가명정보 및 추가정보에 대한 접근 권한 부여 · 변경 · 말소에 관한 사항

나) 가명정보 및 추가정보가 저장 또는 처리되는 시스템 · 단말의 보호조치에 관한 사항

다) 가명정보 및 추가정보에 대한 접근기록 보관 및 점검에 관한 사항

라) 가명정보 및 추가정보의 보유 기간 및 파기 기준 · 방법에 관한 사항

마) 가명정보의 목적 외 활용 방지 및 재식별 방지 대책에 관한 사항

바) 가명정보 제3자 제공 시 사후관리에 관한 사항

2) 신용정보회사등은 가명정보 및 추가정보에 접근하는 취급자들에 대해 다음의 사항을 포함하는 가명정보보호교육을 연 1회 이상 수행하여야 한다.

가) 가명정보의 목적 외 활용 금지에 관한 사항

나) 가명정보의 재식별 금지에 관한 사항

다) 가명정보 재식별 시 즉시 회수 및 삭제에 관한 사항

3) 신용정보회사등은 다음의 사항을 고려하여 가명정보의 보존기간을 주기적으로 검토하고, 그 적정성 여부를 판단하여 필요시 조정하여야 한다.

가) 추가정보 및 가명정보에 대한 기술적 · 관리적 · 물리적 보호조치 수준

나) 가명정보의 재식별시 정보주체에 미치는 영향

다) 가명정보의 재식별 가능성

라) 가명정보의 이용목적 및 그 목적 달성에 필요한 최소기간

4) 신용정보회사등은 가명정보를 통계작성, 연구, 공익적 기록보존 등을 위하여 제공하는 경우 개인신용정보의 제공 · 활용에 대한 동의에 관련 의무(「신용정보법」 제32조제1항 내지 제5항)가 적용되지 않는다(「신용정보법」 제32조제6항 제9호의2). 제3자에게 제공하는 경우 다음의 사항을 준수하여야 한다.

가) 가명정보를 불특정 다수에게 공개하지 아니할 것

나) 가명정보 제공 시 가명정보를 제공 받는 자, 가명정보 활용목적, 가명정보 이용·보존기간 등을 구체적으로 명시하여 제공할 것

다) 가명정보의 재식별 금지, 가명정보의 목적 외 사용 금지 등 관련 법령 준수에 관한 사항을 주지시킬 것

라) 추가정보를 제공하거나 공개하지 않을 것

마) 가명정보의 재식별 가능성을 발견한 경우에는 즉시 그 정보를 처리하고 있는 자에게 통지하고 처리중단 요구 및 해당정보를 회수 · 파기하는 조치를 취할 것

◎ 「신용정보법」 제32조(개인신용정보의 제공 · 활용에 대한 동의)

① 신용정보제공 · 이용자가 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 다음 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공할 때마다 미리 개별적으로 동의를 받아야 한다. 다만, 기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성 · 최신성을 유지하기 위한 경우에는 그러하지 아니하다.

1. 서면
2. 「전자서명법」 제2조제3호에 따른 공인전자서명이 있는 전자문서(「전자문서 및 전자거래 기본법」 제2조제1호에 따른 전자문서를 말한다)
3. 개인신용정보의 제공 내용 및 제공 목적 등을 고려하여 정보 제공 동의의 안정성과 신뢰성이 확보될 수 있는 유무선 통신으로 개인비밀번호를 입력하는 방식
4. 유무선 통신으로 동의 내용을 해당 개인에게 알리고 동의를 받는 방법. 이 경우 본인 여부 및 동의 내용, 그에 대한 해당 개인의 답변을 음성녹음하는 등 증거자료를 확보 · 유지하여야 하며, 대통령령으로 정하는 바에 따른 사후 고지절차를 거친다.
5. 그 밖에 대통령령으로 정하는 방식

② 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사 또는 신용정보집중기관으로부터 개인신용정보를 제공받으려는 자는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 제1항 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공받을 때마다 개별적으로 동의(기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성 · 최신성을 유지하기 위한 경우는 제외한다)를 받아야 한다. 이 경우 개인신용정보를 제공받으려는 자는 개인신용정보의 조회 시 개인신용평점이 하락할 수 있는 때에는 해당 신용정보주체에게 이를 고지하여야 한다.

③ 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사 또는 신용정보집중기관이 개인신용정보를 제2항에 따라 제공하는 경우에는 해당 개인신용정보를 제공받으려는 자가 제2항에 따른 동의를 받았는지를 대통령령으로 정하는 바에 따라 확인하여야 한다.

④ 신용정보회사등은 개인신용정보의 제공 및 활용과 관련하여 동의를 받을 때에는 대통령령으로 정하는 바에 따라 서비스 제공을 위하여 필수적 동의사항과 그 밖의 선택적 동의사항을 구분하여 설명한 후 각각 동의를 받아야 한다. 이 경우 필수적 동의사항은 서비스 제공과의 관련성을 설명하여야 하며, 선택적 동의사항은 정보제공에 동의하지 아니할 수 있다는 사실을 고지하여야 한다.

⑤ 신용정보회사등은 신용정보주체가 선택적 동의사항에 동의하지 아니한다는 이유로 신용정보주체에게 서비스의 제공을 거부하여서는 아니 된다.

다. 보호대책의 준용

그 밖에 신용정보회사등이 마련해야 할 가명정보에 대한 보호조치는 「신용정보업감독규정」 [별표 3]의 신용정보의 기술적 · 관리적 · 물리적 보안대책을 준용한다. 가명정보 및 추가정보의 보호에 관하여 「신용정보업감독규정」 [별표 3]과 신용정보업감독규정 [별표 8]이 경합하는 때에는 [별표 8]을 우선 적용한다.


1234 5678 2345 678
******

Ⅲ. 익명처리 및 적정성 평가

Ⅲ. 익명처리 및 적정성 평가

1. 개 요

가. 익명처리

신용정보회사등은 신용정보법에 따라 더 이상 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 익명처리한 후 이를 회사 내부에서 이용하거나 제3자에게 제공할 수 있다.

나. 익명처리 절차

1) 익명처리

정보집합물(데이터셋)에서 개인을 식별할 수 있는 요소를 전부 또는 일부 삭제하거나 대체하는 등의 방법을 활용하여 더 이상 특정 개인인 신용정보주체를 알아볼 수 없도록 조치한다.

2) 적정성 평가

다른 정보와 결합하여 더 이상 특정 개인인 신용정보주체를 알아볼 수 없도록 적절하게 익명처리하였는지 평가한다. 신용정보회사등은 금융위원회에 익명처리 적정성 심사를 요청할 수 있다.

다. 익명처리에 관한 행위 규칙

1) 기록보존의 의무

신용정보회사등은 개인신용정보를 익명처리를 한 경우에는 다음의 조치 기록을 3년간 보존하여야 한다.

① 익명처리한 날짜

② 익명처리한 정보의 항목

③ 익명처리한 사유와 근거

2. 익명처리 방법

가. 익명처리 기법

1) 총계처리, 데이터 삭제, 데이터 범주화, 데이터 마스킹 및 프라이버시 보호모델 등 여러 가지 기법을 단독 또는 복합적으로 활용해야 한다.

2) 각각의 기법에는 이를 구현할 수 있는 다양한 세부기술이 있으며, 데이터 이용 목적과 기법별 장 · 단점 등을 고려하여 적절한 기법 및 세부기술을 선택하고 활용해야 한다.

※ '부록 1. 가명 · 익명처리 기법' 참고

나. 속성 분류 및 익명처리 적용 기준

1) 신용정보회사등은 익명처리의 대상이 되는 정보를 식별자, 개인식별가능정보로 분류한 후 적정한 익명처리 기법을 적용하여야 한다.

※ 익명처리 대상 정보의 분류는 익명처리 목적 및 이용 · 제공 환경 등에 따라 달라질 수 있음

2) 익명처리시 식별자는 삭제하여야 하며, 부득이하게 정보 이용 목적상 필요한 경우에는 적절하게 익명처리를 한 후 이용하여야 한다.

3) 개인식별가능정보 중 개인 식별 가능성이 높은 속성은 그 정도에 맞추어 익명처리 수준을 높이는 등의 조치를 취하여야 한다.

※ k-익명성 모델 등 프라이버시 보호 모델 적용 가능('부록 2. 프라이버시 보호 모델' 참고)

4) 개인식별가능정보 중 개인 식별 가능성이 낮은 속성은 활용 목적, 해당 정보의 특성, 다른 정보와의 결합 등을 고려하여 필요시 동질성 공격, 배경지식 공격 등의 다양한 위험을 제거하기 위하여 추가로 익명처리 기법을 적용하여야 한다.

※ '부록 2. 프라이버시 보호 모델' 참고

[익명처리 예시]

▷ 처리 목적

A 신용카드사가 보유한 카드 매출 정보를 익명처리하여 B 일반사업자에게 제공하고, B 일반사업자는 이를 분석하여 시장 매출 추이 분석에 활용

▷ 처리 대상

A 신용카드사 고객의 신용카드 매출정보

카드 번호	성명	생년월일	성별	추정소득 (천원)	가맹점 주소	업종 분류 (대/중/소)	매출 발생일	매출 발생 시각	매출 금액
3779 4593 3043 3921	홍길동	1987.11.8	남	90,000	서울시 동작구 만양로 19	문화생활 및 레저 / 생활 / 약국	2021.12.1	10:30:45	23,800
…	…	…	…	…	…	…	…	…	…

① 속성 분류

• 카드번호, 성명을 식별자로 구분하고 기타 칼럼을 개인식별가능정보로 구분

② 익명처리 기준 결정

※ 개인이 식별되지 않도록 여러 기법을 중첩 적용

① 식별자 삭제

• 특정 개인을 식별할 수 있는 식별자는 삭제

② 전체 카드매출 데이터에서 샘플링(50%)

• 특정 개인이 정보집합물에 포함되었는지 여부를 알 수 없도록 전체 원본 정보집합물에서 50%를 무작위 샘플링

– 모집단의 표본 추출 기법을 통해 특정 개인의 식별 가능성을 낮출 수 있음

③ 금액, 날짜, 성별, 연령 칼럼에 잡음 추가

• 대상자를 임의로 10개 그룹으로 분류한 후 서로 독립적인 잡음을 금액, 날짜, 성별, 연령 칼럼에 추가

– 1개 잡음을 유추하더라도 각 잡음은 독립적으로 부여되므로 나머지 잡음을 알아낼 수 없음

비중	잡음 #1	노이즈 #2	노이즈 #3	노이즈 #4
	금액	날짜	생년	성별
10%	–30%	–2주차	–4년	남녀 변경
10%	–20%	–2주차	–4년	남녀 변경
10%	–20%	–1주차	–3년	남녀 변경
10%	–10%	–1주차	–2년	(유지)
10%	–10%	(유지)	–1년	(유지)
10%	10%	(유지)	+1년	(유지)
10%	10%	+1주차	+2년	(유지)
10%	20%	+1주차	+3년	(유지)
10%	20%	+2주차	+4년	(유지)
10%	30%	+2주차	+4년	(유지)

④ 각 항목별로 추가 처리 수행

• 이용 목적 및 개인 식별 가능성을 고려하여 각 칼럼을 추가 익명처리

칼럼	추가 처리 현황
생년월일	출생년도 4자리만 제공하고, 1935년생 이하 또는 2010년생 이상은 상 · 하단 코딩 처리
추정소득	연봉의 분포를 고려하여 4단계로 범주화
가맹점주소	세부주소를 시군구 단위로 범주화
날짜	매출발생일의 날짜는 주차로 범주화(2021.12.1. → 48주차) 매출 발생 시각은 분포를 고려하여 8단계로 범주화(10:30:45 → 09시~12시)
금액	앞 2자리만 남기고 반올림 처리 후 99% 범위에서 상 · 하단 코딩

※ 시장 매출 추이 분석 목적상 업종분류는 소분류 단위까지 유지

⑤ k-익명성 모델 적용

• 생년, 성별, 주소, 업종을 개인식별가능성이 높은 개인식별가능정보(준식별자)로 설정하여 k-익명성 보호 모델 적용(k=5)

생년	성별	추정 소득구간	가맹점 지역	업종 분류 (대/중/소)	매출 발생일	매출 발생 시각	매출 금액
1987년	남	4구간	서울시 동작구	문화생활 및 레저 / 생활 / 약국	48주차	09시~12시	24,000
1987년	남	3구간	서울시 동작구	문화생활 및 레저 / 생활 / 약국	48주차	15시~18시	62,000
1987년	남	3구간	서울시 동작구	문화생활 및 레저 / 생활 / 약국	50주차	15시~18시	7,500
1987년	남	1구간	서울시 동작구	문화생활 및 레저 / 생활 / 약국	49주차	12시~15시	4,800
1987년	남	3구간	서울시 동작구	문화생활 및 레저 / 생활 / 약국	30주차	18시~21시	88,000
…	…	…	…	…	…	…	…

⑥ 시장 매출 추이 분석 목적에 맞게 총계(집계) 처리

• 서울시 지역 약국 업종의 12월(48~52주차), 연령, 성별, 시각에 따른 매출 금액 합계

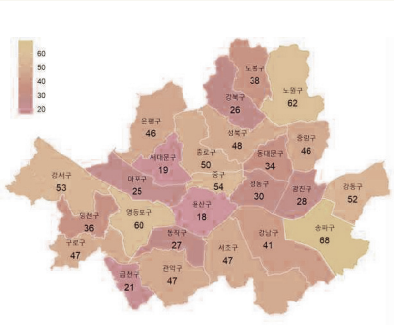
• 특정 업종의 소득구간, 성별에 따른 매출 건수 합계

③ 익명처리 결과

• 서울시 지역별 약국 업종 매출 금액 정보

지역	연령	성별	매출 발생 시각	매출 금액 (천만원)
서울시 동작구	20대	남	09시~12시	5
	20대	여	09시~12시	22
	20대	남	12시~15시	17
	20대	여	12시~15시	29
…	…	…	…	…

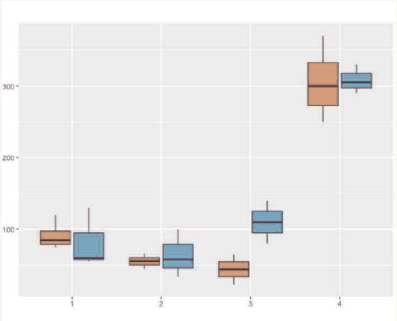
〈서울시 전체 합계〉



• 특정 업종 매출 건수 정보

업종	성별	추정소득 구간	매출 건수
문화생활 및 레저 / 레저 / 테니스장	남	1구간	5
	여	1구간	22
	남	2구간	17
	여	2구간	29
…	…		…

〈매출 건 수 합계〉



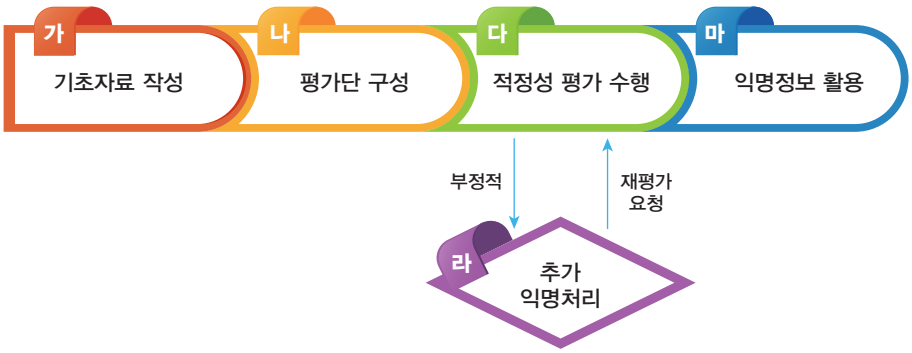
3. 적정성 평가

가. 자체 적정성 평가

신용정보회사등은 익명처리가 적정하게 이루어졌는지 자체적으로 평가를 수행할 수 있으며 다음은 이러한 평가수행 절차의 예시이다.

※ 해당 절차는 예시이며, 신용정보회사등은 자체 규정을 마련하여 수행 가능

〈 (예시) 자체 적정성 평가 수행 절차 〉



가) (기초자료 작성) 신용정보회사등은 적정성 평가에 필요한 데이터 명세, 익명처리 현황, 이용기관의 관리 수준 등이 포함된 기초자료를 작성함

나) (평가단 구성) 신용정보관리 · 보호인이 전문가 3명 이상으로 적정성 평가단을 구성하되, 외부전문가가 평가단의 과반 이상이 되도록 함

※ 평가단 전문가는 '(예시) 적정성 평가위원 자격기준'을 참고하여 구성

다) (적정성 평가 수행) 평가단은 신용정보회사등이 작성한 기초자료와 k-익명성 모델 등을 활용하여 익명처리 수준의 적정성을 평가함

라) (추가 익명처리) 신용정보회사등은 평가결과가 '부적정'인 경우 평가단의 의견을 반영하여 추가 익명처리를 수행한 후 그 적정성을 재평가 받음

마) (익명정보의 활용) 익명처리가 적정하다고 평가받은 경우에는 해당 정보를 이용 또는 제공할 수 있음

〈 (예시) 적정성 평가위원 자격 기준 〉

구분	자격 기준
법률전문가	1. 변호사의 자격을 소지한 자로서 1년 이상 관련 법률 업무(개인정보 보호, 데이터 가공 · 분석 · 활용, 데이터 가명 · 익명처리 및 적정성 평가 등 관련 법률 자문 또는 지원 업무로, 이하 동일)를 수행한 경력이 있는 자 2. 법학박사 학위를 취득한 자로서 2년 이상 관련 법률 업무를 수행한 경력이 있는 자 3. 법학석사 학위를 취득한 자로서 4년 이상 관련 법률 업무를 수행한 경력이 있는 자 4. 법학학사 학위를 취득한 자로서 6년 이상 관련 법률 업무를 수행한 경력이 있는 자 5. 8년 이상 관련 법률 업무를 수행한 경력이 있는 자
기술전문가	1. 국가기술자격법에 따른 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사 자격을 취득한 자로서 2년 이상 관련 업무(개인정보 보호, 데이터 가공 · 분석 · 활용, 데이터 가명 · 익명처리 및 적정성 평가 등으로, 이하 동일)를 수행한 경력이 있는 자 2. 관련 분야(컴퓨터공학, 정보보호학, 데이터베이스공학, 통계학, 수학 등으로, 이하 동일)에서 박사 학위를 취득한 자로서 2년 이상 관련 업무를 수행한 경력이 있는 자 3. 관련 분야에서 석사 학위를 취득한 자로서, 4년 이상 관련 업무를 수행한 경력이 있는 자 4. 관련 분야에서 학사 학위를 취득한 자로서 6년 이상 관련 업무를 수행한 경력이 있는 자 5. 관련 분야에서 8년 이상 관련 업무를 수행한 경력이 있는 자

나. 금융위원회의 적정성 평가 (데이터전문기관 위탁)

신용정보회사등은 「신용정보법」에 따라 개인신용정보에 대하여 익명처리가 적정하게 이루어졌는지 금융위원회에 적정성 심사를 요청할 수 있다.

※ 금융위원회가 적정하게 익명처리가 이루어졌다고 인정한 경우 더 이상 해당 개인인 신용정보주체를 알아볼 수 없는 정보로 추정(개인신용정보에 해당한다는 반증이 없는 한 개인신용정보가 아니지만 개인신용정보라는 반증이 나오는 경우 개인신용정보로 본다는 의미임)

◎「신용정보법」 제40조의2(가명처리 · 익명처리에 관한 행위규칙)

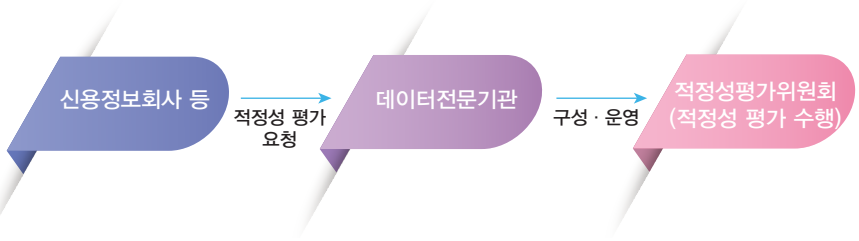
③ 신용정보회사등은 개인신용정보에 대한 익명처리가 적정하게 이루어졌는지 여부에 대하여 금융위원회에 그 심사를 요청할 수 있다.

④ 금융위원회가 제3항의 요청에 따라 심사하여 적정하게 익명처리가 이루어졌다고 인정한 경우 더 이상 해당 개인인 신용정보주체를 알아볼 수 없는 정보로 추정한다.

⑤ 금융위원회는 제3항의 심사 및 제4항의 인정 업무에 대해서는 대통령령으로 정하는 바에 따라 제26조의4에 따른 데이터전문기관에 위탁할 수 있다.

금융위원회는 익명처리 적정성 평가 관련 업무를 「신용정보법 시행령」제37조(권한의 위임 또는 위탁)에 따라 데이터전문기관에 위탁하고 있으며, 데이터전문기관은 가명처리 · 익명처리 관련 기법, 법률 등에 대한 전문지식 수준 등에 따른 자격 기준을 마련하여 적정성 평가위원회를 구성 · 운영할 수 있다.

〈 적정성 평가 절차 〉



적정성 평가를 신청할 경우, 신용정보회사등은 적정성평가위원회가 해당 익명처리의 적정성을 판단할 수 있도록 데이터 명세, 익명처리 현황 등을 포함한 기초자료와 자체 기준 및 절차에 따라 익명처리된 데이터를 제출하여야 한다.

※ 제출해야 하는 신청서 및 기초자료 내용은 '부록 5. 익명처리 적정성 평가 신청서 작성 방법', '부록 7. 익명처리 적정성 평가 기초자료 작성 방법(예시)' 참고

◎「신용정보법」 시행령 제37조(권한의 위임 또는 위탁)

⑤ 금융위원회는 법 제40조의2제3항의 익명처리의 적정성 심사 및 법 제40조의2제4항의 익명처리의 적정성 인정업무를 데이터전문기관에 위탁한다.

금융분야 **가명·익명처리 안내서**

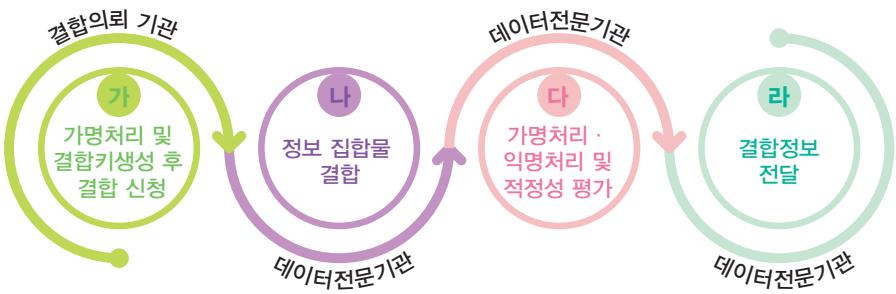
Ⅳ. 정보집합물 결합

Ⅳ. 정보집합물 결합

1. 개 요

개정된 「신용정보법」은 신용정보회사등이 자신이 보유한 정보집합물을 제3자가 보유한 정보집합물을 데이터전문기관을 통하여 결합하는 것을 허용하고 있다.

〈 정보집합물 결합 절차 개요 〉



가. 가명처리 및 결합키 생성 후 정보집합물 결합 신청

결합의뢰기관은 결합 대상 정보집합물을 가명처리한 후 결합의뢰기관간 협의한 방식으로 결합키를 생성하고 데이터전문기관에 정보집합물 결합을 신청한다. 결합의뢰기관은 결합추진 여부를 결정하기 위하여 본 단계 전에 결합률 사전통지*를 데이터전문기관에 의뢰할 수 있다.

* 결합률 사전통지 : 결합의뢰기관간 협의된 방식으로 생성된 결합키를 데이터전문기관이 미리 전달받아, 이를 기준으로 매칭된 결합률을 결합의뢰기관에 통지

※ '결합률 사전통지'는 결합의뢰기관의 선택에 따른 절차로, 데이터전문기관에 따라 결합률 사전통지 서비스를 운영하지 않을 수 있음

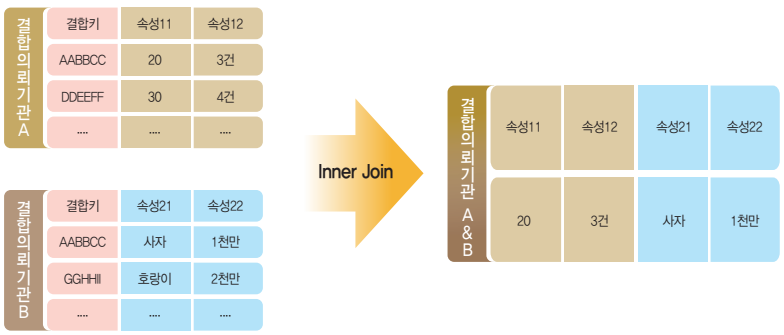
나. 정보집합물 결합

결합의뢰기관은 데이터전문기관에 결합 신청이 접수되면, 결합 대상 정보집합물을 저장매체 또는 정보통신망을 통해 데이터전문기관이 정하는 안전한 방법으로 데이터전문기관에 전달한다. 데이터전문기관은 전달받은 복수의 정보집합물을 결합키를 기준으로 결합*한다.

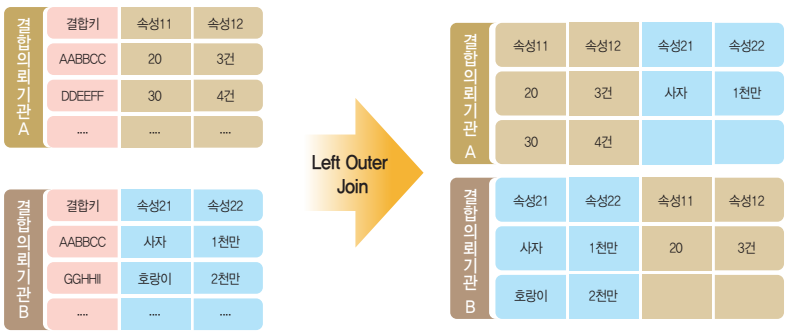
* 데이터전문기관은 결합의뢰기관이 제출한 결합 대상 정보집합물에서 결합키가 같은 레코드의 속성들을 결합하여 결합된 결과물만 양 결합의뢰기관에 전달(Inner Join)하며, 결합되지 않은 결과물은 해당 정보집합물을 전달한 결합의뢰기관에만 전달 가능(Left Outer Join). 단, 결합의뢰기관 책임하에 적정성평가시 이용기관으로 참여한 기관에 제공 가능

〈 (예시) Inner Join 및 Left Outer Join 비교 〉

1. Inner Join



2. Left Outer Join



다. 가명 · 익명처리 및 적정성 평가

데이터전문기관은 결합정보를 결합의뢰기관의 선택에 따라* 가명처리 또는 익명처리를 추가로 수행한 후 적정성 평가를 진행한다. 적정성 평가 결과가 '적정'이 나올 때까지 가명처리 또는 익명처리를 수행한다.

* 결합의뢰기관이 가명정보를 요청한 경우에는 가명처리 및 가명처리 적정성 평가를, 익명정보를 요청한 경우에는 익명처리 및 익명처리 적정성 평가를 수행

※ 데이터전문기관은 신청단계에서 결합의뢰기관의 선택에 따라 결합정보를 가명처리 또는 익명처리한 후 전달 (데이터전문기관이 분석공간을 제공할 경우, 가명 · 익명처리 적정성 평가가 완료된 데이터만 분석할 수 있음. 단, 결합정보를 반출하지 않는 조건 하에서는 가명처리 수준은 다를 수 있음)

라. 결합정보 전달

데이터전문기관은 적정성 평가까지 완료한 결합정보를 결합의뢰기관에 안전한 방법으로 전달(전송)한다. 결합정보가 정상적으로 수신되면 데이터전문기관은 관련 파일 일체를 지체 없이 파기한다.

2. 결합 절차

결합 세부 절차

가. 결합키 생성

결합의뢰기관은 결합 상대기관과 협의한 방식으로 결합키를 생성한 후 결합 대상 정보집합물에 추가한다. 결합의뢰기관은 서로 협의하여 결합키의 생성 알고리즘과 생성시 활용할 입력정보(식별자)를 선택한다. 이 때, 결합키 생성을 위한 입력정보로 주민등록번호는 사용할 수 없으며, 생성된 결합키는 데이터의 신용정보주체를 유일하게 식별할 수 있는 값이어야 한다.

결합의뢰기관은 결합키가 포함된 정보집합물을 데이터전문기관에 안전하게 전달해야 하며, 일방향 해시함수 등 결합키 생성에 관한 정보는 데이터전문기관과 공유할 수 없다. 결합의뢰기관은 생성한 결합키를 상호 공유할 수 없다.

[결합키 생성 방법 예시]

1. 결합키 생성절차

1) 결합의뢰기관은 결합키 생성을 위한 입력정보 및 인코딩 방식을 상호 협의하여 결정하여야 한다.

① 결합의뢰기관 상호 공통으로 보유하고 있는 정보를 활용하여 결합키 생성에 사용될 입력정보를 결정하여야 한다.

※ 예시) 성명 + 휴대폰번호

- 정보집합물 결합을 위한 결합키로 주민등록번호를 사용할 수 없으며, 결합키를 생성하기 위한 입력정보로도 활용할 수 없다(「개인정보 보호법」 제24조의2).
- 결합키 생성을 위해 입력되는 모든 정보는 동일한 방식으로 입력되어야 한다.

② 결합의뢰기관은 원본 정보와 결합시에도 개인을 식별할 수 없도록 ①에서 정한 결합키 입력정보에 솔트값을 추가하여 결합키를 생성하여야 한다.

※ 예시) 솔트값 : 'abcd1234'

③ 결합의뢰기관은 ①에서 정한 입력정보에 성명, 주소 등 한글과 같이 다국어가 포함될 경우 인코딩 방식이 동일해야 하므로 상호 동일한 인코딩(encoding)방식을 정하여 인코딩 한다.

※ 예시) utf-8, euc-kr 등

2) 결합의뢰기관은 결합키 생성 알고리즘 및 결합키 표현방식을 결정한다.

① 결합의뢰기관이 결합키를 생성할 알고리즘(일방향 해시함수 등)을 결정한다.

※ 예시) 일방향 해시함수(SHA256/384/512, HAS-160 등), XOR 등.

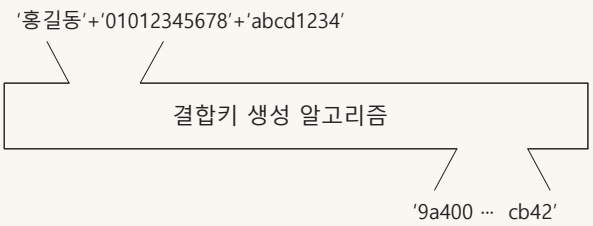
② 결합의뢰기관은 결정된 입력정보와 합의한 알고리즘으로 생성한 결합키의 표현방식을 결정한다.

※ 예시) base64, hexa 등

• 결합의뢰기관은 입력정보의 예시를 활용하여 입력정보와 생성된 결합키를 상호 교환하여 일치 여부를 확인한다.

※ 결합의뢰기관은 결합키 생성방식의 오류 유무를 확인할 때 실제 데이터로 확인하여서는 아니 되며, 기관간 협의된 가짜 데이터를 활용(예 : 실존하지 않는 가상의 인물의 성명, 전화번호 등을 활용)

〈 입력정보 예시 〉



2. 일방향 해시함수를 이용한 결합키 생성 예시

1) 결합의뢰기관은 결합키 생성을 위한 입력정보 및 솔트값을 결정한다.

성명, 생년월일(6자리), 휴대폰번호, 'abcd'

※ 결합의뢰기관 간 공통적으로 보유한 정보중 식별자 칼럼3개, 잡음으로 'abcd'를 선택

2) 결합의뢰기관은 입력정보에 대한 인코딩 방식을 결정한다.

UTF-8

※ 결합키와 정보집합물에 한글 등 다국어가 포함될 경우 결합의뢰기관 간 인코딩 방식을 정함

3) 결합의뢰기관은 결합키를 생성할 알고리즘(일방향 해시함수 등) 및 출력정보에 대한 인코딩 방식을 결정한다.

SHA256(해시함수), HEXA 소문자(출력값 인코딩)

※ 일방향 해시함수의 출력 정보는 이진(binary) 값이므로 텍스트 문자열로 변경하기 위해서는 결합의뢰기관 간 상호 협의하여 인코딩 방식을 정함

4) 결합의뢰기관은 예시를 통해 결합키를 생성하고 결합의뢰기관 간 상호 교환하여 결합키 일치 여부를 확인한다.

〈 결합키 생성 예시 〉

'홍길동8012120101234 1234abcd'

↓ UTF-8

SHA256()

↓ hexa

'9a4005ebbdc5b5dcf399e1905c4291b48bdafb8549308eca84610b14f556cb42'

※ SHA256함수의 출력(32바이트)을 hexa로 표현하면 64바이트임

나. 가명처리

결합의뢰기관은 안내서에 따라 결합 대상 정보집합물의 가명처리를 수행한다.

다. 결합신청서 제출

정보집합물 결합을 희망하는 복수의 결합의뢰기관은 정보집합물 결합 신청서를 데이터전문기관에 각각 제출하여야 한다.

※ 본 안내서 '부록 4. 정보집합물 결합 신청서 작성 방법' 참고

- 결합의뢰기관은 신청서를 제출할 때 결합 대상 정보집합물의 기초자료*를 첨부하여야 함
  * 결합 대상 정보집합물의 정보(이름, 크기, 행과 열의 수 등) 및 칼럼별 정보(데이터 유형, 데이터 길이 등)가 포함되어야 함

※ 본 안내서 '부록 6. 정보집합물 결합 기초자료 작성 방법(예시)' 참고

- 결합의뢰기관이 결합정보를 가명정보로 수신하고자 하는 경우 이용 목적 및 보호조치 수준과 관련된 자료*를 첨부하여야 함
  * 관련 자료는 감독기관 검사 등에 대비하여 보관할 것을 권고

※ 본 안내서 '부록 8. 결합정보 관리 환경 및 이행확약서 작성 방법' 참고

※ 결합률 사전통지는 결합의뢰기관이 선택적으로 활용하는 절차로서, 결합의뢰기관은 해당 절차를 거치지 않고 '사. 정보집합물 전달(전송)' 절차를 바로 진행할 수 있음(데이터전문기관에 따라서는 결합률 사전통지 제도를 운영하지 않을 수 있으므로 사전 확인 필요)

라. 결합률 사전통지 신청

결합의뢰기관은 정보집합물 결합의 효과를 검토하기 위하여 정보집합물 결합 신청서를 작성하여 데이터전문기관에 제출한다.

※ 각 결합의뢰기관은 신청서를 개별 제출하여야 한다.

마 결합키 전달(전송)

각 결합의뢰기관은 결합률 사전통지 신청이 접수되면 결합키를 데이터전문기관에 안전한 방법으로 전달(전송)한다.

바. 결합률 사전통지 수신

데이터전문기관은 전달받은 결합키의 일치여부를 확인하여 결합률을 산출하고 그 결과를 결합의뢰기관에게 통지한다.

◎ 데이터 설명회

▶ 데이터전문기관은 결합 대상 정보집합물의 구조를 이해하고 가명처리 수준을 확인하기 위해 결합의뢰기관으로부터 데이터에 대한 설명을 듣는 데이터 설명회를 진행할 수 있으며 주기적·반복적 결합 등 데이터에 대한 추가 설명이 필요없다고 판단한 경우 데이터 설명회를 생략할 수 있음

사. 정보집합물 전달(전송)

결합의뢰기관은 전문기관과 협의*하여 결합 대상 정보집합물을 저장매체 또는 정보통신망을 이용하여 데이터전문기관에 전달한다.

* 전문기관별로 정보집합물 전달방법이 상이할 수 있으므로 사전에 협의 필요

※ 결합의뢰기관은 정보집합물이 아래의 내용을 담은 CSV 형식이 되도록 하여야 함

▶ 헤더(칼럼명) + 레코드(결합키, 속성1, 속성2, 속성3, 속성4...)

〈 예 시 〉

헤더(칼럼명)	→	key, val0, val1, val2, val3, val4
레코드 1	→	ASEDF111, 2000, 15.4, 3000, 240, 100
레코드 2	→	485DDDKK, 4200, 15.2, 5000, 250, 150
...		...

아. 정보집합물 결합

데이터전문기관은 정보집합물을 결합한 후 결합의뢰기관의 선택에 따라 가명처리 또는 익명처리를 수행하고 적정성 평가를 진행한다.

- 데이터전문기관은 가명 · 익명처리 목적, 가명정보 이용기관의 재식별 의도 및 능력, 가명정보 보호 수준 및 신뢰도 분석 등을 고려하여 가명처리 또는 익명처리의 적정성을 평가
- 데이터전문기관은 결합 완료후 결합키를 삭제 또는 대체*

  * 결합정보 내 신용정보주체 구분, 주기적 · 반복적 정보집합물 결합시 신용정보주체별 연결 등을 위해 필요한 경우 연결키를 생성하여 결합키를 대체

자. 결합정보 전달(전송)

데이터전문기관은 적정성 평가가 완료된 결합정보를 안전한 방법으로 전달(전송)한다.

- 결합정보가 정상적으로 수신되면 데이터전문기관은 결합의뢰기관의 확인을 거쳐 관련 파일 일체를 파기하고, 파기되었음을 결합의뢰기관에 안내

◎ **데이터전문기관의 분석 시스템 이용**

▶ 데이터전문기관이 분석 시스템을 운영하는 경우, 결합의뢰기관은 데이터전문기관의 승인을 받아 분석 시스템에 보유 데이터를 반입하거나 분석결과를 반출할 수 있음

① **(분석공간 신청)** 결합의뢰기관은 결합정보를 데이터전문기관의 분석 시스템에서 분석하고자 할 경우, 결합정보 수신 전 데이터전문기관에 분석공간 이용을 신청

- **(보유 데이터 반입)** 결합의뢰기관이 보유 데이터와 결합정보를 함께 분석하고자 할 경우, 보유 데이터에 대한 반입을 신청

② **(결합정보 분석)** 결합의뢰기관은 결합정보 및 반입한 보유 데이터 등을 분석하여 이용목적을 충족하기 위한 분석결과를 도출

③ **(분석결과 반출)** 결합의뢰기관이 분석결과의 반출심사를 신청하고 데이터전문기관이 이를 승인하면 결합의뢰기관은 분석결과를 반출하여 이용목적에 맞게 활용 가능

④ **(관련 파일 일체 파기)** 결합의뢰기관의 분석결과 반출 후 데이터전문기관은 관련 파일 일체를 파기

⑤ **(반출입 기록 저장)** 데이터전문기관은 결합의뢰기관의 결합 관련 기록과 함께 결합의뢰기관의 분석공간 활용 및 데이터 반출입 기록을 저장하고 관리

차. 결합정보 활용 및 사후관리

결합의뢰기관은 결합정보를 가명정보로 수신한 경우, 신청 단계에서 기재한 이용 목적에 한하여 활용하고 이에 대한 철저한 보호조치*를 수행하여야 한다.

* 본 안내서 'Ⅱ. 5. 가명정보 및 추가정보에 관한 보호조치 기준' 참고

※ 익명정보의 경우 목적 제한 없이 자유롭게 활용 가능하여 보호조치 불요

- 결합의뢰기관은 가명정보 보호조치 등 사후관리를 수행*

  * 금융분야 결합의뢰기관 및 이용기관은 「신용정보법」, 비금융분야 결합의뢰기관 및 이용기관은 「개인정보 보호법」 등 관련 법령에 따라 사후관리 수행

- 결합의뢰기관이 영리 또는 부정한 목적을 위하여 특정 개인을 알아볼 수 있게 결합정보 재결합하는 등 가명정보를 처리하는 것은 엄격히 금지됨(「신용정보법」 제40조의2제6항)

- 결합정보는 정보집합물 결합 신청시 결합정보를 이용할 기관으로 명시하지 않은 제3자에게 제공하는 것은 금지됨

  ※ (사례) 정보집합물 결합시 결합의뢰기관 A, B가 결합정보를 이용기관 C에게 제공하였는데, 추후 C가 D에게 결합정보를 임의로 제공하는 것은 데이터전문기관이 해당 정보집합물 결합 및 적정성 평가시 고려하지 않은 사항으로서 허용되지 않음(결합의뢰기관 A, B가 데이터전문기관에 새로 정보집합물 결합을 신청하고 D의 가명정보 활용 목적, 보호수준 등을 고려한 적정성 평가를 수행 후 제공해야 함)

3. 데이터전문기관 보유 정보집합물과 외부 정보집합물과의 결합

전문기관이 보유한 정보집합물과 외부 기관의 정보집합물을 결합하는 경우 결합목적, 결합정보 이용기관, 관련 대가 지급 여부 등을 종합적으로 고려하여 이해상충 발생가능성이 없어야 한다.

가. 결합목적

결합할 정보집합물을 보유한 데이터전문기관의 이익과 관련 여부 등을 보아 판단한다.

나. 이용기관

결합 대상 정보집합물을 보유한 데이터전문기관과 결합정보를 이용하는 기관과의 연관성 등을 보아 판단한다.

다. 대가지급

데이터전문기관이 자체 보유 정보집합물과 외부기관의 정보집합물을 결합하여 결합정보를 해당 외부기관에 전달시 자체 데이터 가공 및 결합 등 해당 업무처리에 소요된 실비 등의 범위 내에서 외부기관 등으로부터 대가를 받았는지 여부 등을 보아 판단한다.

4. 주기적 · 반복적 정보집합물 결합 및 활용

가. 개요

신용정보회사등이 제3의 기관과 정보집합물 결합을 추진할 때 추후 동일한 상대기관, 동일한 활용목적, 동일한 형태의 정보집합물을 주기적 · 반복적으로 결합할 필요가 있는 경우*에 해당한다. 이에 해당하는 경우, 신용정보회사등은 데이터전문기관에 정보집합물 결합을 의뢰할 때 정보집합물 결합 신청서에 주기적 · 반복적 정보집합물 결합 신청과 관련된 내용을 함께 제출하여야 한다.

* 시계열 분석, 장기적 연구, 주기적 통계처리 등

〈 주기적 · 반복적 정보집합물 결합 관련 고려사항 〉

항 목	고려사항
활용 목적	• 최초 결합과 동일한 목적으로 활용하여야 함
정보 구조	• 최초 결합정보와 동일한 정보 구조(칼럼 구성 등)를 유지하여야 함
이용 환경	• 최초 결합정보와 동일한 이용자가 활용하여야 함
연결키 생성	• 데이터전문기관은 결합 후 결합정보를 파기하고 연결키 생성 알고리즘, 솔트값 등을 보유 * 주기적 · 반복적 결합을 통해 시간순의 데이터 추가 등이 가능
주기적 · 반복적 결합 기간*	• 주기적 · 반복적 결합에 대한 기한 명시 필요(기한이 완료되면 데이터전문기관은 연결키 생성 알고리즘, 솔트값 등을 파기)

* 데이터전문기관이 대내외적인 환경 변화로 인해 주기적 · 반복적 업무처리가 불가능하다고 판단한 경우 주기적 · 반복적 업무처리 종료 및 관련 데이터 파기 가능

주기적 · 반복적 정보집합물 결합시 결합정보를 신용정보주체별로 연결해야 할 필요가 있는 경우 데이터전문기관은 연결키를 생성하여 결합키를 대체한다.* 데이터전문기관은 적정성 평가 완료 후 결합정보를 결합의뢰기관에 전달하고 연결키 생성정보**를 이용한 경우에는 그 정보를 분리 보관하여야 한다.

* 신용정보주체별로 연결될 필요가 없는 경우에, 데이터전문기관은 결합키를 대체하지 않고 삭제

** 연결키 생성 알고리즘, 솔트값 등

결합의뢰기관은 전달받은 결합정보를 연결키를 기준으로 연결하여 활용할 수 있다.

나. 주기적 · 반복적 정보집합물 결합 절차

1) 최초 정보집합물 결합

결합의뢰기관은 정보집합물 결합 신청시 주기적 · 반복적 정보집합물 결합을 함께 신청한다. 데이터전문기관은 정보집합물 결합 후 결합키를 삭제 또는 대체하고 적정성 평가를 완료한 후 결합정보를 결합의뢰기관에게 전송한다.

2) 이후 주기적 · 반복적 정보집합물 결합

결합의뢰기관은 정보집합물 결합 신청시 주기적 · 반복적 정보집합물 결합을 함께 신청한다. 최초 결합시 결합의뢰기관이 결합키를 대체한 경우, 두 번째 결합부터는 최초 정보집합물 결합 때 저장했던 연결키 생성정보를 이용하여 연결키를 생성하고 결합키를 대체한다. 데이터전문기관은 적정성 평가를 완료한 후 결합정보를 결합의뢰기관에게 전송한다.

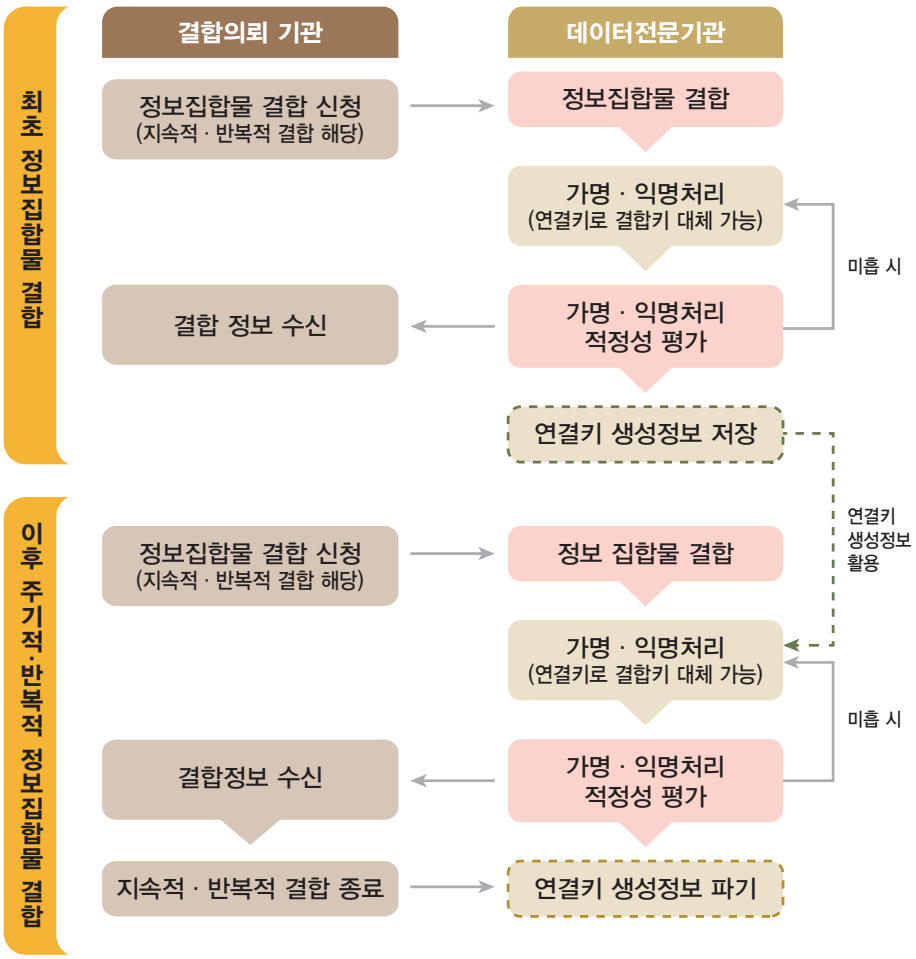
3) 주기적 · 반복적 정보집합물 결합 종료시

결합의뢰기관은 주기적·반복적 정보집합물 결합이 종료될 경우, 데이터전문기관에 통지*하여야 한다. 주기적·반복적 정보집합물 결합이 종료되면 데이터전문기관은 해당 주기적·반복적 결합 건에 대한 연결키 생성정보 등을 파기**하여야 한다.

* 마지막 주기적 · 반복적 정보집합물 결합 신청시 신청기간에 '종료예정일' 입력

** 결합키를 대체한 경우에 해당

〈 주기적 · 반복적 정보집합물 결합 절차 〉




1234 5678 2345 678
******

부 록

부록1 가명·익명처리 기법

◎ 『가명정보 처리 가이드라인』(개인정보보호위원회, '21.10월), ISO/IEC 20889, 「한국신용정보원 가명처리 · 익명처리 전문가 양성」 연수자료 등 참조

◎ 개별 기법의 세부설명 및 적용예시는 『가명정보 처리 가이드라인』(개인정보보호위원회, '21.10월)의 '참고자료를 참고하고, 아래 기술 분류 중 '프라이버시 보호 모델'은 본 안내서 '부록 2. 프라이버시 보호 모델' 참고

◎ 신용정보회사등은 가명·익명처리시 본 안내서에서 설명하는 기술 중 적합한 기술을 선별하여 적용하여야 하며, 필요시 여러 세부기술을 중첩 적용하여 재식별 위험성을 낮추어야 함

◎ 본 안내서에서 설명하지 않은 다른 기술이 더 적합하다고 판단될 경우에는 법령을 위반하지 않는 범위 내에서 해당 기술을 적용할 수 있음

분류	기술	세부기술	설명
개인정보 삭제	삭제기술	삭제 (Suppression)	• 원본정보에서 개인정보를 단순 삭제
		부분삭제 (Partial suppression)	• 개인정보 전체를 삭제하는 방식이 아니라 일부를 삭제
		행 항목 삭제 (Record suppression)	• 다른 정보와 뚜렷하게 구별되는 행 항목을 삭제
		로컬 삭제 (Local suppression)	• 특이정보를 해당 행 항목에서 삭제

분류	기술	세부기술	설명
개인정보 일부 또는 전부 대체	삭제기술	마스킹 (Masking)	• 특정 항목의 일부 또는 전부를 공백 또는 문자 (‘ * ’, ‘ _ ’ 등이나 전각 기호)로 대체
	통계도구	총계처리 (Aggregation)	• 평균값, 최댓값, 최솟값, 최빈값, 중간값 등으로 처리
		부분총계 (Micro aggregation)	• 정보집합물 내 하나 또는 그 이상의 행 항목에 해당하는 특정 열 항목을 총계처리. 즉, 다른 정보에 비하여 오차 범위가 큰 항목을 평균값 등으로 대체
	일반화 (범주화) 기술	일반 라운딩 (Rounding)	• 올림, 내림, 반올림 등의 기준을 적용하여 집계 처리하는 방법으로, 일반적으로 세세한 정보보다는 전체 통계정보가 필요한 경우 많이 사용
		랜덤 라운딩 (Random rounding)	• 수치 데이터를 임의의 수인 자리 수, 실제 수 기준으로 올림(round up) 또는 내림(round down)하는 기법
		제어 라운딩 (Controlled rounding)	• 라운딩 적용 시 값의 변경에 따라 행이나 열의 합이 원본의 행이나 열의 합과 일치하지 않는 단점을 해결하기 위해 원본과 결과가 동일하도록 라운딩을 적용하는 기법
		상 · 하단코딩 (Top and bottom coding)	• 정규분포의 특성을 가진 데이터에서 양쪽 끝에 치우친 정보는 적은 수의 분포를 가지게 되어 식별성을 가질 수 있음 • 이를 해결하기 위해 적은 수의 분포를 가진 양 끝단의 정보를 범주화 등의 기법을 적용하여 식별성을 낮추는 기법
		로컬 일반화 (Local generalization)	• 전체 정보집합물 중 특정 열 항목(들)에서 특이한 값을 가지거나 분포상의 특이성으로 인해 식별성이 높아지는 경우 해당 부분만 일반화를 적용하여 식별성을 낮추는 기법
		범위 방법 (Data range)	• 수치 데이터를 임의의 수 기준의 범위(range)로 설정하는 기법으로, 해당 값의 범위 또는 구간(interval)으로 표현

분류	기술	세부기술	설명
개인정보 일부 또는 전부 대체	일반화 (범주화) 기술	문자데이터 범주화 (Categorization of character data)	• 문자로 저장된 정보에 대해 보다 상위의 개념으로 범주화하는 기법
	암호화	양방향 암호화 (Two-way encryption)	• 특정 정보에 대해 암호화와 암호화된 정보에 대한 복호화가 가능한 암호화 기법 • 암호화 및 복호화에 동일 비밀키로 암호화하는 대칭키(Symmetric key) 방식과 공개키와 개인키를 이용하는 비대칭키(Asymmetric key) 방식으로 구분
		일방향 암호화 – 암호학적 해시함수 (One-way encryption – Cryptographic hash function)	• 원문에 대한 암호화의 적용만 가능하고 암호문에 대한 복호화 적용이 불가능한 암호화 기법 • 키가 없는 해시함수(MDC, Message Digest Code), 솔트(Salt)가 있는 해시함수, 키가 있는 해시함수 (MAC, Message Authentication Code)로 구분 • 암호화(해시처리)된 값에 대한 복호화가 불가능하고, 동일한 해시 값과 매핑(mapping)되는 2개의 고유한 서로 다른 입력 값을 찾는 것이 계산상 불가능하여 충돌 가능성이 매우 적음
		순서보존 암호화 (Order-preserving encryption)	• 원본정보의 순서와 암호값의 순서가 동일하게 유지되는 암호화 방식 • 암호화된 상태에서도 원본정보의 순서가 유지되어 값들 간의 크기에 대한 비교 분석이 필요한 경우 안전한 분석이 가능
		형태보존 암호화 (Format-preserving encryption)	• 원본 정보의 형태와 암호화된 값의 형태가 동일하게 유지되는 암호화 방식 • 원본 정보와 동일한 크기와 구성 형태를 가지기 때문에 일반적인 암호화가 가지고 있는 저장 공간의 스키마 변경 이슈가 없어 저장 공간의 비용 증가를 해결할 수 있음 • 암호화로 인해 발생하는 시스템의 수정이 거의 발생하지 않아 토큰화, 신용카드 번호의 암호화 등에서 기존 시스템의 변경 없이 암호화를 적용할 때 사용

분류	기술	세부기술	설명
개인정보 일부 또는 전부 대체	암호화	동형 암호화 (Homomorphic encryption)	• 암호화된 상태에서의 연산이 가능한 암호화 방식으로 원래의 값을 암호화한 상태로 연산 처리를 하여 다양한 분석에 이용가능 • 암호화된 상태의 연산값을 복호화 하면 원래의 값을 연산한 것과 동일한 결과를 얻을 수 있는 4세대 암호화 기법
		다형성 암호화 (Polymorphic encryption)	• 가명정보의 부정한 결합을 차단하기 위해 각 도메인별로 서로 다른 가명처리 방법을 사용하여 정보를 제공하는 방법 • 정보 제공 시 서로 다른 방식의 암호화된 가명처리를 적용함에 따라 도메인별로 다른 가명정보를 가지게 됨
	무작위화 기술	잡음 추가 (Noise addition)	• 개인정보에 임의의 숫자 등 잡음을 추가(더하기 또는 곱하기)하는 방법
		순열(치환) (Permutation)	• 분석 시 가치가 적고 식별성이 높은 열 항목에 대해 대상 열 항목의 모든 값을 열 항목 내에서 무작위로 순서를 변경하여 식별성을 낮추는 기법 • 개인정보를 다른 행 항목의 정보와 무작위로 순서를 변경하여 전체정보에 대한 변경 없이 특정 정보가 해당 개인과 연결되지 않도록 하는 방법
		토큰화 (Tokenisation)	• 개인을 식별할 수 있는 정보를 토큰으로 변환 후 대체함으로써 개인정보를 직접 사용하여 발생하는 식별 위험을 제거하여 개인정보를 보호하는 기술 • 토큰 생성 시 적용하는 기술은 의사난수생성 기법이나 양방향 암호화, 형태보존 암호화 기법을 주로 사용
		(의사)난수생성기 ((P)RNG, (Pseudo) Random Number Generator)	• 주어진 입력값에 대해 예측이 불가능하고 패턴이 없는 값을 생성하는 메커니즘으로 임의의 숫자를 개인정보와 대체

분류	기술	세부기술	설명
프라이버시 보호 모델		k-익명성 모델 (k-anonymity model)	• 동일한 속성을 가지는 레코드가 최소 k개 이상 존재하도록 하여 프라이버시를 보호
		l-다양성 모델 (l-diversity model)	• 동질집합(equivalent class)의 민감속성정보(sensitive attribute)가 최소 l개의 다양한 속성을 가지도록 하여 k-익명성의 취약점(동질성 공격, 배경지식 공격)을 보완함
		t-근접성 모델	• 특정 동질집합의 기타속성자 분포와 전체 데이터의 기타속성자 분포 차이를 t 이하가 되도록 조정
		차분 프라이버시 (Differential privacy)	• 특정 개인에 대한 사전지식이 있는 상태에서 데이터베이스 질의(Query)에 대한 응답 값으로 개인을 알 수 없도록 응답 값에 임의의 숫자 잡음(Noise)을 추가하여 특정 개인의 존재 여부를 알 수 없도록 하는 기법 • 1개 항목이 차이나는 두 데이터베이스 간의 차이(확률분포)를 기준으로 하는 프라이버시 보호 모델
가명 · 익명처리를 위한 다양한 기술 (기타 기술)		표본추출 (Sampling)	• 데이터 주체별로 전체 모집단이 아닌 표본에 대해 무작위 레코드 추출 등의 기법을 통해 모집단의 일부를 분석하여 전체에 대한 분석을 대신하는 기법
		해부화 (Anatomization)	• 기존 하나의 데이터셋(테이블)을 식별성이 있는 정보집합물과 식별성이 없는 정보집합물로 구성된 2개의 데이터셋으로 분리하는 기술
		재현데이터 (Synthetic data)	• 원본과 최대한 유사한 통계적 성질을 보이는 가상의 데이터를 생성하기 위해 개인정보의 특성을 분석하여 새로운 데이터를 생성하는 기법
		동형비밀분산 (Homomorphic secret sharing)	• 식별정보 또는 기타 식별가능정보를 메시지 공유 알고리즘에 의해 생성된 두 개 이상의 쉐어(share)*로 대체 * 기밀사항을 재구성하는데 사용할 수 있는 하위 집합

부록2 프라이버시 보호 모델

프라이버시 보호 수준을 통계적 기법을 활용하여 정량적으로 나타내는 방식으로, 개인이 직접 식별되는 것뿐만 아니라 추론을 통해 식별되는 것도 방지하는 것을 목적으로 한다. 주로 익명처리 기법으로 활용된다.

가. k-익명성 모델

- 동일한 속성을 가지는 레코드가 최소한 k개 이상 존재하도록 하여 프라이버시를 보호(k=3일 경우, 동일한 개인식별가능정보 중 식별가능성이 높은 정보를 가지는 사람이 3명 이상 존재하여 특정 개인 식별이 불가)

〈 k-익명성 모델 적용 전 〉

[식별자 제거 데이터]			연결공격 (Linkage Attack) 1:01	[확보된 공개 데이터]		
연령	성별	카드 결제금액		이름	연령	성별
60	남	320,000	⟷	김철수	60	남
62	여	600,000	⟷	이민아	62	여
61	남	500,000	⟷	안상태	61	남
27	남	1,500,000	⟷	김상우	27	남
29	남	1,000,000	⟷	한기범	29	남
27	여	1,750,000	⟷	장아름	27	여
26	여	1,400,000	⟷	양수지	26	여
60	여	150,000	⟷	김다래	60	여
61	남	145,000	⟷	윤영하	61	남
60	여	402,000	⟷	김순자	60	여
28	남	1,330,000	⟷	김민영	28	남
25	여	1,220,000	⟷	유슬아	25	여

〈 k개(3개) 이상의 레코드가 존재하는 동질집합을 구성하여 1:1 연결 방지 〉

	[k-익명성 적용 데이터]				[확보된 공개 데이터]		
	연령	성별	카드 결제금액	k : 1	이름	연령	성별
동질집합 (EquivalentClass)	60대	남	320,000		김철수	60	남
	60대	남	500,000		이민아	62	여
	60대	남	145,000		안상태	61	남
	60대	여	600,000		김상우	27	남
	60대	여	150,000		한기범	29	남
	60대	여	402,000		장아름	27	여
	20대	남	1,500,000		양수지	26	여
	20대	남	1,000,000		김다래	60	여
	20대	남	1,330,000		윤영하	61	남
	20대	여	1,750,000		김순자	60	여
	20대	여	1,400,000		김민영	28	남
	20대	여	1,220,000		유슬아	25	여

- k-익명성 모델의 취약점
  - 동질성 공격(Homogeneity attack): k-익명성에 의해 레코드들이 범주화 되었더라도 일부 정보들이 모두 같은 값을 가질 수 있기 때문에 데이터 집합에서 동일한 정보를 이용하여 공격 대상의 정보를 알아내는 공격
  - 배경지식에 의한 공격(Background knowledge attack): 주어진 데이터 이외의 공격자의 배경지식을 통해 공격 대상의 민감한 정보를 알아내는 공격(예를 들어, 여자는 전립선염에 걸릴 수 없다는 배경지식을 활용하여 개인정보 추론)

◎ **원인**

▶ 다양성의 부족(lack of diversity)

▶ 조치 시 정보의 다양성을 고려하지 않음(동일한 정보를 가진 레코드가 하나의 동질집합으로 구성될 경우 동질성 공격에 무방비)

▶ 강한 배경지식(strong background knowledge) : 의료, 금융, 교육 등 영역별 전문지식

나. l-다양성 모델

• 동질집합(equivalent class)의 민감속성정보(sensitive attribute)가 최소한 l개의 다양한 속성을 가지도록 하여 k-익명성의 취약점(동질성 공격, 배경지식 공격)을 보완함

〈 l-다양성 모델 적용 전 〉

[K-익명성 적용 데이터]

연령	성별	우편번호	신용등급
60대	남	180**	8
60대	남	180**	8
60대	남	180**	8
60대	남	180**	8
60대	여	180**	1
60대	여	180**	3
60대	여	180**	5
60대	여	180**	2

동질성 공격 (Homogeneity Attack)

ㅇㅇㅇ지역의 모든 60대 남자의 신용등급은 8등급
(추론 예) ㅇㅇㅇ지역에 사는 남자, 박철수의 신용등급은 8등급

↓

동질집합 내에서 다양성이 부족하여 특정 개인의 정보 추론 가능

〈 l-다양성 모델 적용 후 〉

동질집합이 l개(3개)의 다양한 민감정보(신용등급)을 가지도록 조정

[l-다양성 적용 데이터]

연령	성별	우편번호	신용등급
60대	*	1803*	8
60대	*	1803*	8
60대	*	1803*	5
60대	*	1803*	2
60대	*	1804*	1
60대	*	1804*	3
60대	*	1804*	8
60대	*	1804*	8

60대 남자의 신용등급 추론 가능성 낮아짐
(l값= 3)

• l-다양성 모델의 취약점

– 쏠림 공격(skewness attack): 정보가 특정한 값에 쏠려 있는 경우 l-다양성 모델이 프라이버시를 보호하지 못함

◎ 쏠림 공격의 예

▶ 임의의 동질집합이 99개의 '위암 양성', 1개의 '위암 음성' 레코드로 구성되어 있다고 가정

▶ 공격자는 공격 대상이 99%의 확률로 '위암 양성'이라는 것을 알 수 있음

– 유사성 공격(similarity attack) : 익명처리된 레코드의 정보가 서로 비슷하다면 l-다양성 모델을 통해 처리되었다 할지라도 프라이버시가 노출될 수 있음

◎ 유사성 공격의 예

▶ 동질 집합의 병명이 서로 다르지만 의미가 유사할 수 있음(위궤양, 급성위염, 만성위염)

▶ 이를 통해, 공격자는 공격 대상의 질병이 '위'에 관련된 것이라는 사실을 알아낼 수 있음

다. t-근접성 모델

• 특정 동질집합의 개인식별가능정보 분포와 전체 데이터의 개인식별가능정보 분포 차이를 t 이하가 되도록 조정(t가 0에 가까울수록 분포가 유사하며, 이를 통해 특정집단의 개인식별가능정보 추론문제 보완)

〈 t-근접성 모델 적용 전 〉

[l-다양성 적용 데이터]

연령	성별	우편번호	소득
60대	남	180**	10,000
60대	남	180**	50,000
60대	남	180**	60,000
60대	남	180**	15,000
60대	여	180**	35,000,000
60대	여	180**	100,000,000
60대	여	180**	175,000,000
60대	여	180**	24,000,000

쏠림 공격
(Skewness Attack)

ㅇㅇㅇ지역의 60대 남자의
소득은 매우 낮다
(추론 예) ㅇㅇㅇ지역에 사는 남자,
박철수의 소득은 매우 낮다
↓
특정한 값에 쏠린 특성을 이용하여
개인의 정보 추론 가능

〈 t-근접성 모델 적용 후 〉

[t-근접성 적용 데이터]

연령	성별	우편번호	소득
60대	*	1803*	10,000
60대	*	1803*	50,000
60대	*	1803*	175,000,000
60대	*	1803*	24,000,000
60대	*	1804*	35,000,000
60대	*	1804*	100,000,000
60대	*	1804*	60,000
60대	*	1804*	15,000

기타속성자 분포의 특성을
이용한 추론 방지

60대 남자의 소득수준
추론 가능성 낮아짐

참 고

임의의 동질 집합에서 민감한 분포 Pec, 전체 데이터에 대한 민감한 정보의 분포 Q

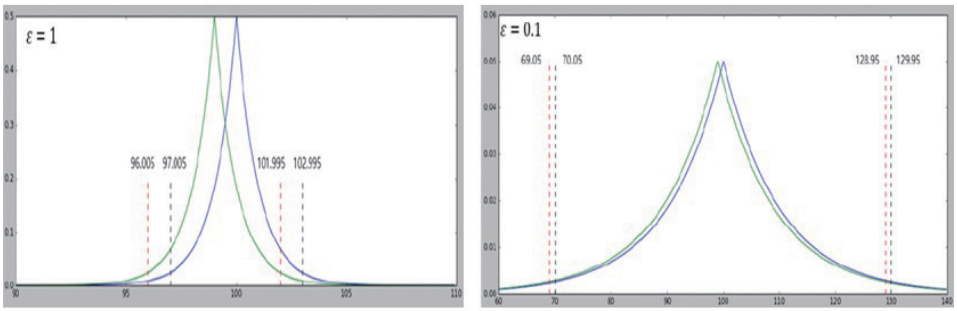
– 모든 동일 집합에 대하여 Pec와 Q의 차이(D[Pec, Q]) t를 계산

– 분포의 차이가 t 이하여야 한다는 정의에 따라, 가장 큰 분포의 차이값이 전체 데이터의 t근접성을 대표함

라. 차분 프라이버시 보호 모델(differential privacy)

- k-익명성, l-다양성의 취약한 부분을 보완하기 위해 C.Dwork가 제안한 모형
- 1개의 레코드가 차이 나는 두 DB의 차이(확률 분포)를 기준으로 하는 프라이버시 모델
  - 두 DB간에 차이가 존재하면 차분 공격으로 알 수 있으나, 차이가 일정 크기 이하면 k>2 처럼 프라이버시 보호 수준이 생김
  - 샘플링 또는 노이즈 추가 : 차이를 줄이기 위한 조치
  - ε : 차이의 크기

$$P[K(D_1)\in S] \le \exp(\varepsilon)\times P[K(D_2)\in S] \text{ for all } S \subseteq Range(K)$$



Laplace(라플라스) 분포

원본

개인식별가능정보			신용불량여부
직업	성별	나이	
비-기술직	남자	[30~60)	Yes=2, No=17
전문직	남자	[30~60)	Yes=3, No=17
전문직	남자	[1~30)	Yes=1, No=20
전문직	여자	[30~60)	Yes=3, No=12
기술직	여자	[60~90)	Yes=2, No=23

[1/4 분기]

개인식별가능정보			신용불량여부
직업	성별	나이	
비-기술직	남자	[30~60)	Yes=1, No=17
전문직	남자	[30~60)	Yes=3, No=17
전문직	남자	[1~30)	Yes=1, No=20
전문직	여자	[30~60)	Yes=3, No=12
기술직	여자	[60~90)	Yes=2, No=23

[2/4 분기]

노이즈(샘플링 또는 가짜 레코드 삽입) 처리 후

개인식별가능정보			신용불량여부
직업	성별	나이	
비-기술직	남자	[30~60)	Yes=2+3, No=17+2
전문직	남자	[30~60)	Yes=3-1, No=17-2
전문직	남자	[1~30)	Yes=1+3, No=20+4
전문직	여자	[30~60)	Yes=3+5, No=12-3
기술직	여자	[60~90)	Yes=2+4, No=23+5

[1/4 분기]

개인식별가능정보			신용불량여부
직업	성별	나이	
비-기술직	남자	[30~60)	Yes=1+4, No=17+3
전문직	남자	[30~60)	Yes=3-2, No=17+1
전문직	남자	[1~30)	Yes=1+4, No=20+4
전문직	여자	[30~60)	Yes=3-1, No=12-2
기술직	여자	[60~90)	Yes=2+3, No=23+4

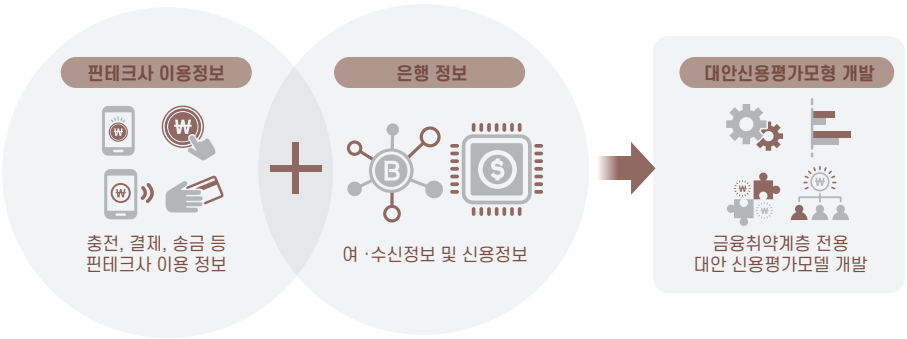
[2/4 분기]

출처: 공주대 최대선 교수

부록3 가명 · 익명정보 활용 사례

1. 가명정보 결합 및 활용 사례

가. 핀테크 결제 · 고객 행동 정보 ✚ 은행 여 · 수신정보
➡ 청년층 신용평가 모형 개발



주요데이터

결제정보, 송금정보, 충전정보, 대출정보, 연체정보, 부동산정보, 소득정보 등

• 활용

청년층이 다수 이용하는 핀테크 사의 고객 행위정보(충전, 결제, 송금 등)와 은행의 여 · 수신 및 신용정보를 결합하고 결합정보를 분석하여 청년층을 위한 대안신용평가모형 개발

• 기대효과

대안신용평가모형을 바탕으로 금융 이력이 부족하여 금융 접근성이 낮은 청년층에게도 다양한 금융상품 및 금융서비스 제공

나. 화물차 운행량 · 안전운행 정보 ✚ CB사의 운전자 신용정보 ➡ 화물차 안전 운전자 맞춤형 신용평가 모델 연구

주요데이터

차종, 교통사고 건수, 고속도로 미납요금 횟수, 운행거리, 운행시간, 위험운전행동 건수, 연령대, 성별, 연체보유여부, 신용등급 등

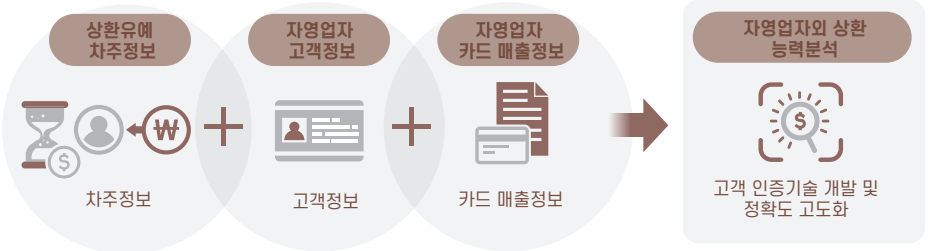
- **활용**

  교통 공공기관이 보유한 개인 화물차의 운행량 및 안전운행 정보와 CB사의 신용정보를 결합하고 결합정보를 분석하여 안전운전 사업자에 대한 맞춤형 신용평가모델 개발

- **기대효과**

  안전운전 사업자에 대한 맞춤형 신용평가 모델을 바탕으로 운수업 종사자에 대한 신용대출 조건 개선 등 금융 지원 활성화

다. 만기연장 · 상환유예 차주정보 ✚ 자영업자 차주 정보 ✚ 자영업자 카드 매출정보 ✚ 자영업자 신용정보약 ➡ 자영업자의 상환 능력 분석



주요데이터

만기연장 상환유예 유형, 연체 금액, 부도 사유, 월 매출액, 신용 점수, 대출 잔액 등

- **활용**

  만기연장 및 상환유예 정보와 매출정보 결합으로 코로나19로 인한 자영업자 지원 프로그램 종료 이전 취약 자영업자의 상환능력 분석

- **기대효과**

  코로나19로 인한 자영업자의 피해규모 분석 후 정책적 지원

라. 은행 거래정보 ✚ 증권사 투자정보 ✚ 생명보험사 가입정보 ✚ 카드사 결제정보 ✚ 손해보험사 가입정보 ✚ CB사 신용정보 ➡ 기관별 고객 분석 및 금융트렌드 공동연구

주요데이터

거래금액, 거래건수, 결제금액, 결제건수, 자산정보, 평잔수치정보, 카드개설정보, 카드실적정보, 신용점수, 보험가입건수, 보험가입금액, 보장금액, 지급금액 등

- **활용**

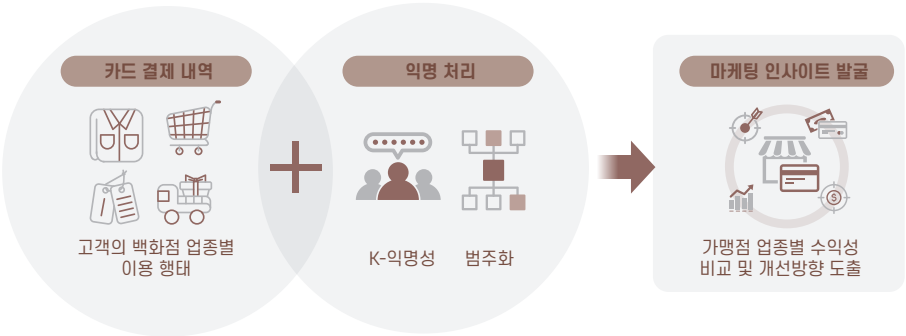
  각 분야별 대표적인 금융사들이 보유하고 있는 독자적인 데이터를 결합 및 분석하여 기관별 고객 관리 및 예측 모형 개발하고 금융 공동지수 연구 등 수행

- **기대효과**

  금융트렌트 공동연구, 신상품 개발 및 마케팅 등에 활용

2. 익명정보 활용 사례

가. 카드 결제 내역을 통한 고객의 백화점 업종별 이용 행태 통계
➡ 고객 분석 및 마케팅 인사이트 발굴



주요데이터

가맹점 업종, 가맹점 지역코드, 고객 연령대, 고객 소득구간, 업종별 이용 고객 수

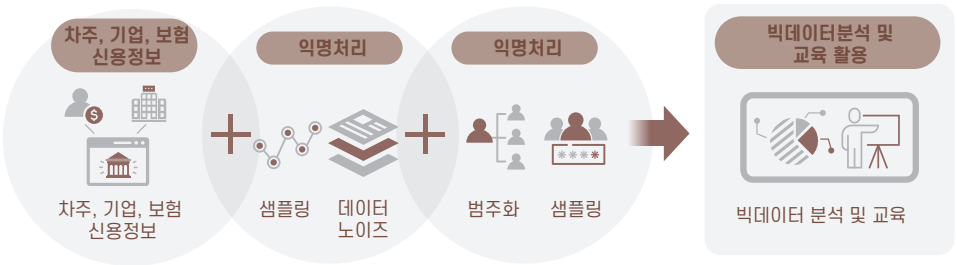
• **활용**

카드사 보유 데이터에 k-익명성, 범주화, 샘플링, 치환 등의 익명처리를 진행하여 개인 식별성을 제거하고 익명정보를 토대로 추정 고객군 분류 및 고객군의 백화점 내 가맹점 이용 횟수 파악

• **기대효과**

고객군의 가맹점 업종별 이용 횟수를 토대로 업종별 수익성 비교 및 개선방안 도출

나. 차주정보, 보험정보, 기업신용정보 ➡ 빅데이터 분석 및 교육 활용



주요데이터

연체 금액, 연체 사유 코드, 납입 보험료, 보험 종류 코드, 수익 전망 등급, 기업 규모 코드 등

• **활용**

① 샘플링 후 신용정보 이력이 많은 상위 20% 이내 대상자 제외 ② 금액/날짜/성별/연령에 랜덤 노이즈를 부여 ③ 각 항목별로 민감도에 따라 추가 익명처리(범주화, 상단코딩 등) 수행 ④ 추가 샘플링 후 분석 자료 및 교육자료로 제공

• **기대효과**

신용정보를 익명처리하여 빅데이터 분석 교육 및 데이터 구조 파악에 활용

다. 증권사 투자정보 및 생명보험사 보험정보 ➡ 빅데이터 분석 공모전 제공

주요데이터

주식자산정보, 매수금액, 보유종목수, 거래종목수, 보험가입금액, 월납보험료, 보험 수익률 등

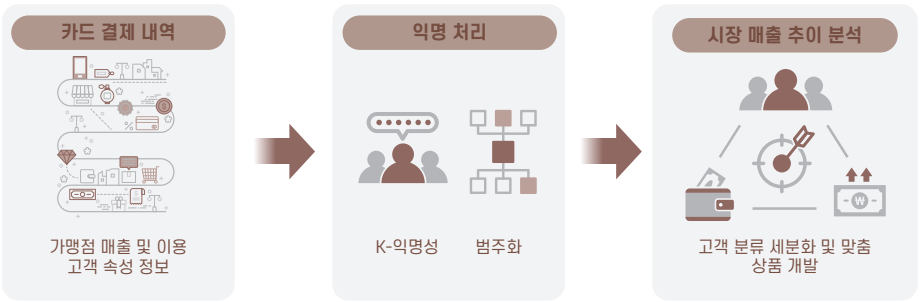
- **활용**

  고객의 거리패턴, 자산보유, 서비스 이용 내역 등의 데이터를 분석하여 고객에게 필요한 서비스를 제안하는 빅데이터 공모전에 데이터셋 제공

- **기대효과**

  금융 빅데이터에 관심이 있는 학생들이 실제로 데이터를 직접 다뤄보며 실무를 접할 수 있는 기회를 제공하고 신사업 발굴할 수 있는 정보를 제공

라. 카드 결제 내역을 통한 가맹점 매출 및 이용 고객 속성 정보
➡ 시장 매출 추이 분석 및 맞춤 상품 개발



주요데이터

가맹점 업종, 매출 발생 일자, 고객 연령대, 고객 소득구간, 일인가구 추정 회원수, 반려동물 양육 추정 회원수, 매출금액

- **활용**

  카드사 보유 데이터에 k-익명성, 범주화, 로컬 삭제 등의 익명처리를 진행하여 개인 식별성을 제거하고 익명정보를 토대로 특정 품목을 구매한 고객군 파악

- **기대효과**

  구매 내역을 토대로 각 품목에 따른 매출 추이 분석 및 특정 고객군에 대한 맞춤 상품 개발

부록4 정보집합물 결합 신청서 작성 방법

① 정보집합물 결합 신청서

② 접수번호	*미기재*		접수일	*미기재*	
결합의뢰 기관명	기관명		담당자(성명,직함)		
	담당부서		전화번호		
	소재지		이메일 주소		
③ 결합상대 기관명 (복수기재 가능)	기관명				
	담당부서				
	소재지				
④ 결합목적	*☐ 결합률 사전통지 신청 ☐ 주기적·반복적 여부 ☐ 분석 시스템 이용 여부* *결합목적을 구체적으로 서술*				
⑤ 정보집합물 주요내용 요약	*간략히 서술*				
⑥ 결합 데이터 제공형태	☐ 가명정보	이용목적	☐ 통계작성 (상업적 목적 포함) ☐ 연구 (산업적 연구 포함) ☐ 공익적 기록보존 등		
		결합키	☐ 삭제 ☐ 대체		
	☐ 익명정보				

「신용정보의 이용 및 보호에 관한 법률」 제17조의2제1항에 따라 위와 같이 신청합니다.

년 월 일

⑦ 신청인 (서명 또는 인)

(전문기관명)장 귀하

⑧ 첨부서류	정보집합물의 데이터 명세서

① 정보집합물 결합 신청서 작성

• (작성 주체) 결합 신청서는 신청기관별로 각자 제출

② 접수번호 및 접수일

• 데이터전문기관에서 관리하는 항목으로써, 공란으로 제출

③ 결합상대 기관명(복수 기재 가능)

• 참여하는 모든 기관의 정보 입력

– 결합 상대 기관이 2개 이상일 경우, 복수로 기재

④ 결합목적

• 정보집합물 결합 신청 목적을 구체적 기재함과 더불어 아래 사항에 대한 내용 추가 기입

– (이용 주체) 결합 데이터를 이용하는 기관명 모두 기재

[예시]

※ 이용기관 : ○○사, △△사(제3자 제공)

– (결합 방식) 데이터 결합 방식에 대한 설명 기재

[예시]

※ ○○사 데이터를 기준으로 ㅁㅁ사 데이터 Left Join

◎ (결합률 사전통지 신청) 결합률 사전통지를 희망하는 경우 해당 항목을 기입 후 확인 목적을 작성

※ (목적 예시) 내부 시스템 고도화를 위해 ○○사와 ㅁㅁ사 데이터를 결합한 가명결합 데이터 구축 전, 사전 결합 매칭률 확인

※ (정보집합물 주요내용 예시) 사전결합률 분석용 결합키

◎ (주기적 · 반복적 업무) 주기적 · 반복적 결합이 필요한 경우 해당 항목을 기입 후 관련 내용을 작성

※ 본 안내서 'Ⅳ. 4. 주기적 · 반복적 정보집합물 결합 및 활용' 참고

※ (예시) – 신청 차수 : 최초
– 신청 주기 : 분기별
– 종료 예정일 : 20XX.XX.XX
– 활용 목적, 데이터 구조 및 이용 환경 동일

◎ (분석 시스템 이용) 데이터전문기관의 전산설비 등을 활용하여 분석을 희망하는 경우 해당 항목을 기입 후 관련 내용을 작성

※ 해당 데이터전문기관 이용 안내서 참고

※ (예시) 결합 데이터 전송(전달) 없이 데이터전문기관의 원격 데이터 분석센터 이용

⑤ 정보집합물 주요내용 요약

• 결합 데이터에 대한 주요 내용을 간략하게 서술

⑥ 결합 데이터 제공 형태

• 최종 산출된 결합 데이터의 제공 형태

– (가명정보) 결합 데이터의 이용목적 및 결합키* 삭제 여부 확인

* 결합키는 삭제가 원칙, 신용정보주체별 연결 작업 필요시 연결키로 대체(본 안내서 'Ⅳ. 2. 결합절차 – 정보집합물 결합' 참고)

– (익명정보) 추가 기입 사항 없음

⑦ 신청인 서명날인

• 신청 기관의 신용정보관리 · 보호인, CISO 및 CPO 등 이에 준하는 책임자급 이상 직원의 서명 날인

⑧ 첨부서류

• 결합 신청자 유형에 따른 추가 제출 서류는 아래의 표와 같음

– 데이터 제공 : 정보집합물의 데이터 명세서

– 데이터 이용* : 결합정보 관리 환경 및 이행 확약서

* 가명정보로 이용 신청 시 제출

구 분	데이터 제공 및 이용	데이터 제공	데이터 이용
정보집합물의 데이터 명세서	O	O	
결합정보 관리 환경 및 이행 확약서	O		O

부록5 익명처리 적정성평가 신청서 작성 방법

익명처리 적정성 평가 신청서

① 접수번호	*미기재*		접수일	*미기재*
평가의뢰 기관명	기관명		담당자(성명,직함)	
	담당부서		전화번호	
	소재지		이메일 주소	
② 활용목적	*□ 주기적·반복적 여부* *간략히 서술 (예시: 내부활용, 제3자 제공, 불특정 다수에게 공개)*			
③ 정보집합물 주요내용 요약	*간략히 서술 (예시: 16년 9월 A카드사의 카드 매출 정보)*			

「신용정보의 이용 및 보호에 관한 법률」 제26조의4제2항제2호에 따라 위와 같이 신청합니다.

년 월 일

④ 신청인 (서명 또는 인)

(전문기관명)장 귀하

첨부서류	정보집합물의 데이터 명세서

① 접수번호 및 접수일

• 데이터전문기관에서 관리하는 항목으로써, 공란으로 제출

② 활용목적

• 데이터전문기관에서 평가의 참고 목적을 위해 익명처리 적정성 평가 이후 활용 목적을 간략히 기재

◎ (주기적 · 반복적 업무) 주기적 · 반복적 결합이 필요한 경우 해당 항목을 기입 후 관련 내용을 작성

※ (예시) – 신청 차수 : 최초

– 종료 예정일 : 20XX.XX.XX

– 활용 목적, 데이터 구조 및 이용 환경 동일

③ 정보집합물 주요내용 요약

• 평가 대상 데이터에 대한 주요 내용을 간략하게 서술

④ 신청인 서명날인

• 신청 기관의 신용정보관리 · 보호인, CISO 및 CPO 등 이에 준하는 책임자급 이상 직원의 서명 날인

부록6 정보집합물 결합 기초자료 작성 방법(예시)

1. 기초자료 작성 항목

데이터 명세	• 개요(의뢰기관명, 데이터 용량, 활용 목적, 이용기관 등)
	• 정보 개요(정보영역, 항목건수, 비중 등)
	• 정보 항목별 상세(항목 설명, 분포현황 포함 여부, 예시 등)
가명처리 요약	• 데이터 전체 적용
	• 데이터 칼럼별 적용
범주형 변수 분포현황	• 칼럼명, 세부설명, 빈도수, 구성비 등
수치형 변수 분포현황	• 칼럼명, 분위수 등

※ 분량 제한 없음

2. 기초자료 개요(작성예시 포함)

가. 데이터 명세

1) 결합 관련 개요

항목	내용
의뢰기관명	*A카드*
데이터 크기 (용량)	*20.5 GB*
데이터 레코드 수	*25,000,000*
데이터 칼럼 수	*14*
데이터 생성 방법	*18년~20년 A카드 이용자에 대한 카드상품 신청/이용/탈퇴 등의 내부정보 및 외부 조회 정보*
결합정보 활용목적	*B은행의 신규 신용카드 결합상품 개발시 참고하기 위한 통계작성*
결합정보 이용기관	*B은행*

2) 정보 개요

정보영역	항목건수	비중
KEY	1	7.1%
신청정보	6	42.9%
결제정보	2	14.3%
대출정보	2	14.3%
기타정보	3	21.4%
Total	14	100%

• 정보영역 : 데이터 항목별 대분류 정보를 의미

3) 정보 항목별 상세(정보집합물 전체 항목에 대해 작성)

정보원천	자료형	정보영역	칼럼명	항목명(국문)	항목 설명	분포현황 작성	예시
KEY	–	결합키	A_key	–	작성 불요		
내부정보	수치형	신청정보	col2	연령			90
내부정보	범주형	신청정보	col3	성별			남
내부정보	범주형	신청정보	col4	직업코드		○	20201
내부정보	수치형	신청정보	col5	신청일자			20180101
내부정보	수치형	신청정보	col6	계좌개설일자			20180101
내부정보	수치형	신청정보	col7	개설상품 건수		○	14
내부정보	수치형	결제정보	col8	KK카드상품 결제금액	A카드의 KK카드상품	○	70000
내부정보	수치형	결제정보	col9	MM카드상품 결제금액	A카드의 MM카드상품	○	70000
외부정보	수치형	대출정보	col10	카드대출 상환액	전체 카드대출상품	○	500000
외부정보	수치형	기타정보	col11	소득금액		○	500000
외부정보	수치형	기타정보	col12	건강보험료납부액		○	500000
외부정보	수치형	기타정보	col13	지방세납부액		○	500000

- 정보원천 : 내 · 외부 정보 구분
- 자료형 : 범주형 / 수치형 자료 구분

  - 범주형 : 몇 개의 범주로 나누어진 자료를 의미
    - 명목형 : 단순히 분류된 데이터로 성별, 직업코드, 혈액형 등을 의미
    - 순서형 : 개개의 값들이 이산적이며 그들 사이에 순서 관계가 존재하는 데이터로 연령 등을 의미
  - 수치형 : 이산형과 연속형으로 이루어진 자료를 의미
    - 이산형 : 이산적인 값을 갖는 데이터로 대출건수 등을 의미
    - 연속형 : 연속적인 값을 갖는 데이터로 대출금액 등을 의미

- 칼럼명 : 결합 대상 정보집합물의 실제 칼럼명
- 항목명(국문) : 칼럼명이 영문인 경우 해당 항목의 국문명
- 항목 설명 : 결합 대상 정보집합물의 칼럼에 대한 세부 설명
- 분포현황 작성 : 민감 또는 주요 정보 항목에 대하여 분포 현황 작성 여부

나. 가명처리 요약

- 데이터 전체 적용 : 데이터 전반에 가명처리했을 경우 작성

  ※ (예시) 샘플링 적용, 노이즈 추가 등

가명처리 방법(데이터전체)		
가명처리	**대상 칼럼**	**설명**
샘플링	*전체 데이터*	*전체 데이터 80% 샘플링 적용*

- 데이터 칼럼별 적용 : 가명처리했을 경우에만 처리방법을 작성하며 처리 방식이 여러 개일 경우 셀 추가하여 작성

  ※ 가명처리를 적용하지 않은 경우, 미적용 사유를 작성

칼럼명	가명처리 방법				
	가명처리1	단위/기준	가명처리2	단위/기준	미적용 사유
A_key	작성 불요				
col2	상단코딩	90			
col3					성별 소비패턴이 반드시 필요하여 미적용
col4					
col5					내부 원본정보이므로 분리되면 재식별 위험성 낮음
col6					내부 원본정보이므로 분리되면 재식별 위험성 낮음
col7					내부 원본정보이므로 분리되면 재식별 위험성 낮음
col8	라운딩 (절삭)	10000			
col9		10000			
col10		10000	상단코딩	500000	
col11		10000	상단코딩	500000	
col12		10000	상단코딩	500000	
col13		10000	상단코딩	500000	

칼럼명	데이터 요약					
	(전)원본 Max	(전)원본 Max 빈도수	(후)처리후 min	(후)처리후 min빈도수	(후)처리후 Max	(후)처리후 Max 빈도수
A_key	작성 불요					
col2	99	1			90	10
col3	–					
col4	20201	160			20201	160
col5	–					
col6	–					
col7	–					
col8	77,985	2			70,000	123
col9	77,985	3			70,000	123
col10	222,000,000	2			500000	12,312,312
col11	222,000,000	3			500000	12,341,234
col12	222,000,000	1			500000	12,345,123
col13	222,000,000	2			500000	12,121,212

다. 범주형 변수 분포현황

※ 최종 제출하는 데이터 중 민감 또는 주요 정보에 대하여 작성하며, 추가 작성 요청이 있을 수 있음

칼럼명	항목명(국문)	칼럼값	세부 설명	빈도수	구성비
col4	직업코드	20201	금융업	160	13.95%
		20202	건설업	170	14.82%
		20203	서비스업	153	13.34%
		20204	유통업	160	13.95%
		20205	정보통신업	186	16.22%
		20206	농업	164	14.30%
		20207	수산업	154	13.43%

• 내부에서 사용하는 별도 계층 구조가 있는 데이터의 경우 해당 계층 구조의 설명 자료를 첨부

라. 수치형 변수 분포현황

※ 최종 제출하는 데이터 중 민감 또는 주요 정보에 대하여 작성하며, 추가 작성 요청이 있을 수 있음

칼럼명	최소값	1분위수(25%)	2분위수(중앙값)	3분위 (75%)	최대값
col7	0	5	13	20	25
col8	0	10000	40000	70000	77985
col9	0	10000	40000	70000	77985
col10	0	100000	250000	500000	222000000
col11	0	100000	250000	500000	222000000
col12	0	100000	250000	500000	222000000
col13	0	100000	250000	500000	222000000

• 값의 분포 중에서 특이치가 다수 포함되어 있는 경우 최저 빈도값(개수)과 최고 빈도값(개수)에 대한 설명 자료를 첨부

부록7 익명처리 적정성 평가 기초자료 작성 방법(예시)

1. 기초자료 작성 항목

데이터 명세	• 개요(의뢰기관명, 데이터 용량, 활용 목적, 이용기관 등)
	• 정보 개요(정보영역, 항목건수, 비중 등)
	• 정보 항목별 상세(항목 설명, 분포현황 포함 여부, 예시 등)
익명처리 요약	• 데이터 전체 적용
	• 데이터 칼럼별 적용
범주형 변수 분포현황	• 칼럼명, 세부설명, 빈도수, 구성비 등
수치형 변수 분포현황	• 칼럼명, 분위수 등

※ 분량 제한 없음

2. 기초자료 개요(작성예시 포함)

가. 데이터 명세

1) 익명처리 평가 관련 개요

항목	내용
의뢰기관명	*A카드*
데이터 크기 (용량)	*20.5 GB*
데이터 레코드 수	*25,000,000*
데이터 칼럼 수	*13*
데이터 생성 방법	*19년~20년 A카드 이용자에 대한 카드상품 신청/이용/탈퇴 등의 내부정보 및 외부 스크래핑 정보*
활용목적 (선택)	*A카드 MOU 체결 기관에 A카드 이용정보 제공*

2) 정보 개요

정보영역	항목건수	비중
신청정보	6	46.2%
결제정보	2	15.4%
대출정보	2	7.7%
기타정보	3	23.1%
Total	13	100%

• 정보영역 : 데이터 항목별 대분류 정보를 의미

3) 정보 항목별 상세

정보원천	자료형	정보영역	칼럼명	항목명(국문)	항목 설명	분포현황 작성	예시
내부정보	수치형	신청정보	col2	연령			90
내부정보	범주형	신청정보	col3	성별			남
내부정보	범주형	신청정보	col4	직업코드		○	20201
내부정보	수치형	신청정보	col5	신청일자			20180101
내부정보	수치형	신청정보	col6	계좌개설일자			20180101
내부정보	수치형	신청정보	col7	개설상품 건수		○	14
내부정보	수치형	결제정보	col8	KK카드상품 결제금액	A카드의 KK카드상품	○	70000
내부정보	수치형	결제정보	col9	MM카드상품 결제금액	A카드의 MM카드상품	○	70000
외부정보	수치형	대출정보	col10	카드대출 상환액	전체 카드 대출상품	○	500000
외부정보	수치형	기타정보	col11	소득금액		○	500000
외부정보	수치형	기타정보	col12	건강보험료납부액		○	500000
외부정보	수치형	기타정보	col13	지방세납부액		○	500000

나. 익명처리 요약

1) 데이터 전체 적용 : 데이터 전반에 익명처리했을 경우 작성

※ 예시 : 샘플링 적용, 모델링(K-익명성, L-다양성, t-근접성), 노이즈 추가 등

익명처리 방법(데이터전체)		
익명처리	대상 칼럼	설명
샘플링	*전체 데이터*	*전체 데이터 80% 샘플링 적용*
모델링(K-익명성)	*연령, 성별, 직업코드, 신청일자, 계좌개설일자*	*k=3 적용하여 k=3 미만 레코드 삭제처리*

2) 데이터 칼럼별 적용 : 익명처리했을 경우에만 처리방법을 작성하며 처리 방식이 여러 개일 경우 셀 추가하여 작성

※ 익명처리를 적용하지 않은 경우, 미적용 사유를 작성

칼럼명	개인식별 가능정보	익명처리 방법				
		익명처리 1	단위/기준	익명처리 2	단위/기준	미적용 사유
col2	○	*상단코딩*	*90*			
col3	○					*성별 소비패턴이 반드시 필요하여 미적용*
col4	○	*범주화*				
col5	○					*내부 원본정보이므로 분리되면 재식별 위험성 낮음*
col6	○					*내부 원본정보이므로 분리되면 재식별 위험성 낮음*
col7						*내부 원본정보이므로 분리되면 재식별 위험성 낮음*
col8		*라운딩 (절삭)*	*10000*			
col9			*10000*			
col10			*10000*	*상단코딩*	*500000*	
col11			*10000*	*상단코딩*	*500000*	
col12			*10000*	*상단코딩*	*500000*	
col13			*10000*	*상단코딩*	*500000*	

• 개인식별가능정보 : 개인식별가능정보 해당 여부(용어 정의 참고)

칼럼명	데이터 요약					
	(전)원본 Max	(전)원본 Max 빈도수	(후)처리후 min	(후)처리후 min빈도수	(후)처리후 Max	(후)처리후 Max 빈도수
col2	99	1			90	10
col3	–					
col4	20201	160			20201	160
col5	–					
col6	–					
col7	–					
col8	77,985	2			70,000	123
col9	77,985	3			70,000	123
col10	222,000,000	2			500000	12,312,312
col11	222,000,000	3			500000	12,341,234
col12	222,000,000	1			500000	12,345,123
col13	222,000,000	2			500000	12,121,212

다. 범주형 변수 분포현황

※ 최종 제출하는 데이터 중 민감 또는 주요 정보에 대하여 작성하며, 추가 작성 요청이 있을 수 있음

칼럼명	항목명(국문)	칼럼값	세부 설명	빈도수	구성비
col4	직업코드	20201	금융업	160	13.95%
		20202	건설업	170	14.82%
		20203	서비스업	153	13.34%
		20204	유통업	160	13.95%
		20205	정보통신업	186	16.22%
		20206	농업	164	14.30%
		20207	수산업	154	13.43%

• 내부에서 사용하는 별도 계층 구조가 있는 데이터의 경우 해당 계층 구조의 설명 자료를 첨부

라. 수치형 변수 분포현황

※ 최종 제출하는 데이터 중 민감 또는 주요 정보에 대하여 작성하며, 추가 작성 요청이 있을 수 있음

칼럼명	최소값	1분위수(25%)	2분위수(중앙값)	3분위 (75%)	최대값
col7	*0*	*5*	*13*	*20*	*25*
col8	*0*	*10000*	*40000*	*70000*	*77985*
col9	*0*	*10000*	*40000*	*70000*	*77985*
col10	*0*	*100000*	*250000*	*500000*	*222000000*
col11	*0*	*100000*	*250000*	*500000*	*222000000*
col12	*0*	*100000*	*250000*	*500000*	*222000000*
col13	*0*	*100000*	*250000*	*500000*	*222000000*

• 최소값, 최대값의 경우 빈도수를 포함하여 작성

부록8 결합정보 관리 환경 및 이행확약서 작성 방법

1. 결합정보 관리 환경 체크리스트 개요

가. 개요

데이터전문기관은 결합정보의 가명처리 적정성 평가 목적으로 결합정보 관리 환경 및 이행확약서를 요구할 수 있다.

나. 구성

결합정보 관리 환경 및 이행 확약서는 결합정보의 가명처리 목적, 결합정보 활용 주체 및 이용기관의 가명처리 · 이용 환경을 확인할 수 있는 문항으로 구성되었으며 가명처리 · 이용 환경에 대한 문항은 가명처리에 관한 행위규칙*에서 요구하는 수준으로 작성한다.

* 「신용정보법」 제40조의2(가명처리 · 익명처리에 관한 행위규칙), 「신용정보업감독규정」[별표 8] 가명정보에 관한 보호조치 기준, 「신용정보업감독규정」[별표 3] 기술적 · 물리적 · 관리적 보안대책 마련 기준 외 기타 관련 법령

〈 체크리스트 구성 〉

체크리스트 문항	근거
① 본 신청 건의 결합정보 활용 목적 및 계획	
② 결합정보 활용계획 검토 등에 대한 자체 적정성 심의 절차를 수립했으며, 본 신청 건에 대해 심의 완료	– 금융분야 가명 · 익명처리 안내서 II. 가명처리 2. 가명처리 절차
③ 개인(신용)정보 보호조직을 구성 및 운영	– 개인정보의 안전성 확보조치 기준 제4조
④ 신용정보관리 · 보호인(또는 개인정보보호책임자)을 지정	– 신용정보법 제20조 제3항 – 개인정보보호법 제31조 제1항

체크리스트 문항	근거
⑤ 가명정보 보호를 위해 다음의 항목들을 포함한 내부관리계획을 수립 · 운영	– 신용정보업감독규정[별표8] Ⅱ. 관리적 보호조치 ① – 개인정보보호법 시행령 제29조의5 제1항
⑥ 가명정보 관련 내부관리계획에 대한 이행실태 점검을 연 1회 이상 수행	– 개인정보의 안전성 확보조치 기준 제4조
⑦ 본 건의 결합정보와 원본정보를 분리하여 저장	– 신용정보업감독규정[별표8] Ⅰ. 기술적 · 물리적 보호조치 2. 가명정보에 대한 보호조치 ①
⑧ 결합정보에 대한 기술적인 접근통제 정책 수립	– 신용정보업감독규정[별표8] Ⅰ. 기술적 · 물리적 보호조치 2. 가명정보에 대한 보호조치 Ⅱ. 관리적 보호조치 ①
⑨ 본 건 관련 결합정보 접근 가능 직원이 원본정보에 접근할 수 없도록 권한을 분리하여 운영	– 신용정보업감독규정[별표8] Ⅰ. 기술적 · 물리적 보호조치 2. 가명정보에 대한 보호조치②
⑩ 본 건 관련 결합정보 접근 권한 부여, 변경 또는 말소에 대해 관리자의 승인을 받아 해당 내역을 기록하고, 그 기록을 3년 이상 보관	– 신용정보업감독규정[별표8] Ⅰ. 기술적 · 물리적 보호조치 2. 가명정보에 대한 보호조치 – 신용정보업감독규정[별표3] Ⅱ. 기술적 · 물리적 보안대책 1. 접근통제 2. 접속기록의 위 · 변조방지
⑪ 본 건의 추가정보를 삭제하거나 결합정보와 분리된 저장소에 암호화하여 보관	– 신용정보업감독규정[별표8] Ⅰ. 기술적 · 물리적 보호조치 1. 추가정보에 대한 보호조치 ①
⑫ 가명정보 취급자를 대상으로 다음 항목들을 포함하여 가명정보 보호에 관한 사항을 연 1회 이상 교육 실시	– 신용정보업감독규정[별표8] Ⅱ. 관리적 보호조치 ②
⑬ 다음의 항목들을 고려하여 본 결합정보의 보존 기간을 정하였으며, 보존기간의 적정성을 주기적으로 검토 · 조정	– 신용정보업감독규정[별표8] Ⅱ. 관리적 보호조치 ③
⑭ 가명정보 오 · 남용에 대한 별도 제재기준을 마련	– 신용정보업감독규정[별표8] Ⅰ. 기술적 · 물리적 보호조치 2. 가명정보에 대한 보호조치 ⑥

2. 결합정보 관리 환경 및 이행 확약서 양식(작성방법 및 예시 포함)

결합정보 관리 환경 및 이행 확약서

세부 지표	체크
1 본 신청 건의 결합정보 활용 목적 및 계획 ※ 결합정보 분석 등 처리에 외부 전문가, 자회사, 전자금융보조업자 등을 활용하는 경우에도 '외부 처리 위탁' 선택	□ 내부 활용 □ 외부 처리 위탁 □ 제3자 제공 ※ 복수 체크 가능
세부 내용 (공통) 결합정보 활용 목적 작성 (외부 처리 위탁 체크 시) 위탁사 명, 위탁 처리 내용 작성 (제3자제공 체크 시) 결합정보 제공 받는 회사명, 제공 받는 목적 작성	
<예시> *-(공통) (결합정보 이용기관 A)의 내부 ○○ 정보와 (결합 상대기관 B)의 ○○정보를 결합하여 ○○○○ 목적으로 활용하고자 함* *-(외부 처리 위탁 체크 시) (위탁사 C)에 위탁하여 결합정보를 분석하며, C 직원은 당사에 상주하여 업무 수행*	

2 결합정보 활용계획 검토 등에 대한 자체 적정성 심의 절차를 수립하였으며, 본 신청 건에 대해 심의 완료	□ 예 □ 아니오
세부 내용 자체 적정성 심의 절차가 있는 경우 **본 결합**에 대한 심의 진행 여부와 심의 관련 상세 내용(심의 위원회 구성, 심의 기준 및 결과, 심의 기록 보관 현황 등)에 관해 기술	
<예시> *-당사 내부 적정성 심의 절차에 의해 본 결합에 대한 적정성 심의를 진행하였으며, 해당 결과는 내부 전자결재시스템에 기록 및 보관* *-심의 위원회 구성: ○○부서장, ○○팀장, ○○팀장* *-심의 내용: 본 결합 대상 정보집합물에 대한 가명처리 수준의 적정성, 재식별 가능 여부 등* *-심의 결과: 적정*	

3 개인(신용)정보 보호조직을 구성 및 운영	□ 예 (□ 전담조직 구성) □ 아니오
세부 내용 담당 조직명, 가명정보 생성·처리 및 관리 과정에서 조직의 역할 등에 관해 기술	
<예시> *당사는 개인(신용)정보 보호조직으로 개인정보보호팀을 운영(○명)* *-담당업무: ○○ 업무*	

4 신용정보관리·보호인(또는 개인정보보호책임자)을 지정	☐ 예 (☐ 임원급 이상) ☐ 아니오
세부 내용 신용정보관리·보호인(또는 개인정보보호책임자)의 소속, 지위, 역할, 권한, 겸직 여부 등에 관해 기술	
<예시> *-당사는 내부 ○○○○ 규정에 의거 신용정보관리·보호인을 ○○○으로 지정하고 있음* *-신용정보관리·보호인: ○○○○ 본부장*	

5 가명정보 보호를 위해 다음의 항목들을 포함한 내부관리계획을 수립·운영 1. 가명정보 및 추가정보에 대한 접근 권한 부여·변경·말소에 관한 사항 2. 가명정보 및 추가정보가 저장 또는 처리되는 시스템·단말의 보호조치에 관한 사항 3. 가명정보 및 추가정보에 대한 접근기록 보관 및 점검에 관한 사항 4. 가명정보 및 추가정보의 보유 기간 및 파기 기준·방법에 관한 사항 5. 가명정보 목적 외 활용 방지 및 재식별 방지 대책에 관한 사항 6. 가명정보 제3자 제공 시 사후관리에 관한 사항	☐ 예 ☐ 아니오
세부 내용 내부관리계획 전사 공포 방법, 내부관리계획 제·개정 시 결재권자 등에 관해 기술	
<예시> *-당사는 내부관리계획이 포함된 업무규정을 전직원이 접근가능한 사내 ○○○○에 게시* *-내부관리계획 제·개정시 ○○○○의 결재를 득하여 업무규정에 최종 등재*	

6 가명정보 관련 내부관리계획에 대한 이행실태점검을 연 1회 이상 수행 ※ 가명정보 관련 내용이 추가된 내부관리계획을 기준으로 이행실태점검이 있었던 경우 "예" 선택	☐ 예 ☐ 점검 예정 ☐ 아니오
세부 내용 (공통) 내부관리계획의 이행실태 점검에 대한 최근 이력, 점검 주기, 절차, 사후관리 방안 등에 관해 기술 (점검 예정 체크 시) 이행실태점검 관련 규정 또는 점검 계획 작성	
<예시> *-당사 내부관리계획에 의거하여 이행실태점검 연 ○회 수행* *-점검 수행일: ○○.○○(당해연도)* *-점검 항목:* *-(점검 예정 체크 시) '내부관리계획 제○조 이행실태점검'에 따라 점검할 예정*	

7 본 건의 결합정보와 원본정보를 분리하여 저장 ※ 결합 대상 정보집합물(원본정보)을 제공하지 않고 결합정보를 이용만 하는 경우 "원본정보를 보관하지 않음" 선택	☐ 물리적 분리 ☐ 논리적 분리 ☐ 원본정보를 보관하지 않음
세부 내용 가상머신 분리, 데이터베이스 인스턴스 분리 등 본 건에 대한 구체적인 분리 저장 방안에 관해 기술	
<예시> *-(물리적분리 체크시) 물리적으로 분리된 별도의 DB 서버에 결합정보 보관* *-(논리적분리 체크시) 같은 DB 서버 내 별도의 DB 인스턴스를 생성하여 결합정보 보관* *-(원본정보를 보관하지 않음 체크시) 결합정보를 이용만 하여, 원본정보를 보관하지 않음*	

8 결합정보에 대한 기술적인 접근통제 정책 수립	□ 예 □ 아니오
세부 내용	접근통제 방법, 접근통제 시스템 종류, 접근통제 시스템 권한 관리 방안, 결합정보 접근 단말기에 대한 보호조치, 접근기록 보관(접근자(ID 또는 직원정보 등), 접근 시간)등의 **접근통제 정책 내용에 관해 서술**
<예시> *(접근통제 관련 정책)* *-결합정보 접근 시 서버 접근통제 시스템인 ○○○○을 통해서만 접근 가능* *-서버 접근통제 시스템에 대한 권한은 관리책임자의 승인을 득하면 사내 정보보호팀에서 권한을 부여* *(단말기 관련 정책)* *-결합정보는 전용 단말기에서만 접근 가능* *-전용단말기는 인터넷망과 물리적으로 분리된 전용망에 위치* *(접근기록 보관)* *-○○○○시스템에 가명정보 취급자가 가명정보에 접근한 기록을 보관* *-접근기록은 ○년 간 보관하며, ○○○○팀에서 월 ○회 점검* *-접근기록 내용: 접근자 ID, 접속 IP, 접근 시간, 접근대상 및 접근자 행위 정보*	

9 본 건 관련 결합정보 접근 가능 직원이 원본정보에 접근할 수 없도록 권한을 분리하여 운영	□ 예 □ 아니오
세부 내용	결합정보 접근 가능 직원 인원수 및 소속, 직위 작성 예외적으로 결합정보 접근 가능 직원이 책임자의 승인하에 일시적으로 원본정보에 접근하는 경우 접근 가능 기간 설정, 승인 절차 등에 관해 기술
<예시> *-결합정보 취급자는 원본정보 접근 권한이 없음 (결합정보 취급자: ○○○○팀 과장, ○○○○팀 대리)* *-(예외상황 시 추가기술) 가명정보 취급자가 원본정보 접근이 필요한 경우, 내부전자결재시스템을 통해 관리책임자의 승인을 득하여 일시적으로 부여하고 관련 기록은 3년간 보관*	

10 본 건 관련 결합정보 접근 권한 부여, 변경 또는 말소에 대해 관리자의 승인을 받아 해당 내역을 기록하고, 그 기록을 3년 이상 보관 ※ 행위자, 대상자, 승인자, 변경 정보 포함	□ 예 (□ 전자적 기록) □ 아니오
세부 내용	접근 권한 신청 및 승인 절차, 결재권자, 대상 시스템 및 기록·보관되는 구체적 정보, 보관 기간 등에 관해 기술
<예시> '전자 기록 보관' 선택 *-본 결합정보 취급자: ○○○○팀 과장, ○○○○팀 대리(총 ○명)* *-결합정보 접근 권한 부여 프로세스:* *① 결합정보 취급자는 내부전자결재시스템을 통해 접근 권한 신청* *② 결재권자(○○부서장) 승인* *③ 결재문서는 내부전자결재시스템에 ○년 간 보관* *④ 사내 정보보호팀에서 결합정보 접근 권한을 부여 (접근 허용기간 ○○.○○~○○.○○)* *-접근권한 변경 기록은 ○○접근통제시스템에서 자동 저장 및 보관하며, 해당 기록을 ○○○○팀에서 연 ○회 점검*	

11 본 건의 추가정보를 삭제하거나 결합정보와 분리된 저장소에 암호화하여 보관 ※ 결합 대상 정보집합물(원본정보)을 제공하지 않고 결합정보를 이용만 하는 경우 "추가정보를 보관하지 않음" 선택	□ 추가정보를 보관하지 않음 □ 물리적 분리 □ 논리적 분리
세부 내용	본 결합 대상에 대한 추가정보를 보관하는 경우 그 사유 및 암호화, 분리 보관 방법에 대해 기술
<예시> *- 본 결합 대상의 추가정보는 삭제*	

12 가명정보 취급자를 대상으로 다음 항목들을 포함하여 가명정보 보호에 관한 사항을 연 1회 이상 교육 실시 1. 가명정보의 목적 외 활용 금지에 관한 사항 2. 가명정보의 재식별 금지에 관한 사항 3. 가명정보 재식별 시 즉시 회수 및 삭제에 관한 사항	□ 예 □ 아니오
세부 내용	연간 교육 계획 수립 절차 및 전결권자, 교육 이력 및 교육 계획, 가명정보 관련 커리큘럼* 등에 관해 기술 * 정보보안/개인정보보호 관련 교육에 가명정보 보호에 관한 사항이 포함되어 있을 경우, 해당 과정도 서술 가능
<예시> *- 가명정보 보호에 관한 사항을 가명정보 취급자를 대상으로 하여 연 ○회 교육 실시 (팀 소관)* *- 교육 시행일: ○○.○○* *- 가명정보 교육 내용: 가명정보의 목적 외 활용 금지에 관한 사항, 가명정보의 재식별 금지에 관한 사항, 가명정보 재식별 시 즉시 회수 및 삭제에 관한 사항*	

13 다음의 항목들을 고려하여 본 결합정보의 보존 기간을 정하였으며, 보존기간의 적정성을 주기적으로 검토·조정 1. 추가정보 및 가명정보에 대한 관리적·물리적·기술적 보호조치 기준 2. 가명정보의 재식별 시 정보주체에 미치는 영향 3. 가명정보의 재식별 가능성 4. 가명정보의 이용목적 및 그 목적 달성에 필요한 최소기간	□ 예 □ 아니오
세부 내용	본 결합 대상 가명정보의 보존 기간(파기 시점), 목적 달성 기준, 주기적 재검토 계획 등에 관해 기술
<예시> *-본 결합정보 보존 기간은 결합정보 수신 후 목적 달성까지 기간으로 ○○개월로 지정함 (파기예정일:○○.○○)* *-보존기간의 적정성을 주기적으로 검토하여 보존기간 이전에 목적 달성 시 삭제하거나, 프로젝트 미완료시에는 보존기간을 연장할 계획*	

14 가명정보 오·남용에 대한 별도 제재기준을 마련	□ 예 □ 아니오
세부 내용	오·남용 행위 식별, 제재기준 적용 절차 등에 관해 기술
<예시> *-당사 내부규정 ○○에 가명정보 오남용에 대한 제재기준을 명시*	

본 *(이용기관명)*은 위 사항이 사실과 다르지 않음을 확인하며, *(데이터전문기관)*이 결합하여 제공한 결합정보를 활용함에 있어 「신용정보의 이용 및 보호에 관한 법률」에서 규정하고 있는 가명처리에 관한 행위규칙(감독규정 제43조의7)및 가명정보에 관한 보호조치 기준(감독규정 [별표8])을 성실히 이행하고 기타 관련 법령을 준수하겠습니다.
아울러, 이를 이행·준수하지 아니하여 발생하는 관련 법적 책임을 부담할 것을 확약합니다.

년 월 일

신청인 (서명 또는 인)

(전문기관명)장 귀하

- 위의 항목에 대한 내용을 작성하여 적정성 평가위원회에 제출
- 신청 기관의 신용정보관리 · 보호인, CISO 및 CPO 등 이에 준하는 책임자급 이상 직원의 서명 날인
- 세부 내용 분량 제한 없음
- 세부 내용의 작성예시는 단순 예시일 뿐이며, 결합정보 이용기관 내부 정책에 맞게 작성
- 본 문서는 감독기관 검사 등에 대비하여 가명처리기록과 함께 보관할 것을 권고

부록9 자주하는 질문(FAQ)

1. 가명 · 익명처리

Q1. 가명처리 적정성 평가시 반드시 적정성 평가위원회를 개최해야 하는지?

A
- 가명처리의 경우 평가위원회 개최가 필수는 아니며, 내부 합리적인 자체 기준 및 절차를 수립하여 이행할 수 있으나, 평가위원회를 구성하여 진행하도록 권고

(※ 안내서 Ⅱ.가명처리-2.가명처리 절차-다. 가명처리 적정성 검토 및 추가처리 참고)

Q2. 제3자로부터 제공받은 개인정보도 가명처리할 수 있는지?

A
- 개인정보를 제공한 기관과 체결한 계약 등에 관련 제약사항이 있지 않은 한 가명처리 가능 정보 대상은 제한은 없음

Q3. 기업신용정보도 가명처리의 대상이 되는지?

A
- 개인신용정보가 아닌 경우 가명처리의 대상은 아니지만, 기업신용정보로 보이는 데이터일지라도 그 정보를 구성하는 칼럼의 구체적 내용에 따라 개인이 식별될 수 있으면 개인신용정보에 해당하여 가명처리 필요

Q4. 가명처리의 수준을 어떻게 정해야 하는지? 내부 활용시에도 가명처리를 해야 하는지?

A

- 이용목적, 이용기관(내부활용, 외부제공 등) 등 여러 요인을 종합적으로 고려하여 상황에 따라 가명처리 수준을 달리할 것을 권고
  (※ 본 안내서 Ⅱ.가명처리–3.가명처리 방법–[가명처리 예시] 참고)
- 내부 활용의 경우, 정보집합물이 외부에 노출되는 것이 아니라서 외부 제공하는 경우보다 안전한 환경에서 이용하므로 가명처리 기준이 상대적으로 완화 가능
- 가명정보 접근인력과 원본 및 추가정보 접근인력을 반드시 구분해야 하며, 식별자는 반드시 필요한 경우가 아니면 삭제하고, 내부 활용목적에 필요하지 않은 세부 데이터는 추가 처리 필요(예: 분석목적에 필요하지 않을 경우, 상세주소를 시군구 정보로 대체)

Q5. 결합의뢰기관이 결합 대상 정보집합물에 대해 데이터전문기관에 가명처리를 의뢰할 수 있는지? 가명처리 적정성 평가도 데이터전문기관에 의뢰할 수 있는지?

A

- 데이터전문기관은 원본 데이터에 대한 접근 권한이 없으며, 결합의뢰기관이 데이터전문기관에 가명처리된 상태로 정보집합물을 제공하도록 하고 있으므로, 데이터전문기관이 결합의뢰기관을 대신하여 가명처리를 수행하는 것은 불가능
  (※「신용정보법」 시행령 제14조의2제3항제1호)
- 가명처리는 개별 기관(결합의뢰기관)이 그 적정성 여부를 직접 검토하여야 하며 데이터전문기관의 업무범위에 포함되지 않음
  (※「신용정보법」 제26조의4제2항)

2. 정보집합물 결합

Q6. 결합키를 일방향 해시함수 처리하지 않고 양방향 암호화로 생성해도 되는지?

A

- 관련 법령에서는 결합키 생성 방식을 구체적으로 강제하지는 않으나 결합키 생성방식 채택시 안전성, 보안성, 재식별가능성 등을 충분히 고려하여 결정
  (※ 「신용정보업감독규정」 제15조의2제2항 제2호)

Q7. 사업자등록번호를 추가처리없이 그대로 결합키로 사용할 수 있는지?

A

- 결합키 생성방법은 데이터전문기관이 알 수 없도록 해야하고 (※ 「신용정보업감독규정」 제15조의2 제2항), 사업자등록번호가 다른 데이터와 결합되면 결합정보가 개인(신용)정보로 판단될 수 있으므로 일방향 암호화 등으로 안전하게 추가처리하는 것을 권고)

Q8. 외부결합(OUTER JOIN) 방식으로 정보집합물 결합시 결합되지 않은 데이터도 제공받을 수 있는지?

A

- 외부결합(OUTER JOIN)의 경우 결합의뢰기관이 보유한 데이터를 기준으로 LEFT OUTER JOIN만 가능하며, 결합정보는 해당 결합의뢰기관에게만 제공가능함.
  단, 결합의뢰기관 책임하에 적정성평가시 이용기관으로 참여한 기관에 제공 가능
  (※ 본 안내서 Ⅳ.정보집합물 결합–1.개요–나.정보집합물 결합 참고)

Q9. A기관과 B기관이 결합을 하고 A기관만 결합정보를 이용하겠다고 한 경우, 결합 이후 B기관 인원이 A 기관 건물 내부로 들어와서 결합정보에 대한 데이터 분석을 하는 경우에 대해 문제가 없는지?

A

- 데이터전문기관에서 정보집합물 결합 후 적정성 평가시, 이용기관 담당자로 명시된 사람만 결합정보를 이용할 수 있는 것이 원칙
- 단, A기관 데이터 분석을 위해 타 기관과 위수탁 관계가 있는 경우 적정성 평가시 관련 내용을 명시하고 평가를 받으면 타 기관 담당자(B기관 등)도 결합정보 이용 가능

Q10. 주기적 · 반복적 정보집합물 결합시 최초에 기재하여 제출한 이용목적을 변경 또는 확대하는 것이 가능한지?

A

- 최초 결합과 동일한 목적으로만 주기적 · 반복적 정보집합물 결합을 할 수 있으며, 목적을 변경 또는 확대할 경우에는 새로운 정보집합물 결합으로 다시 신청
  (※ 본 안내서 Ⅳ.정보집합물 결합–4.주기적 · 반복적 정보집합물 결합–가.개요 참고)

Q11. 회사내 정보집합물을 결합 할 경우에도 데이터전문기관을 통해 결합해야하는지?

A

- 내부 정보집합물 결합의 경우는 데이터전문기관을 이용할 필요는 없으며 자체 결합 가능

Q12. 정보집합물 결합 신청 시 결합키는 반드시 1개이어야 하는가?

A

- 결합키는 결합의뢰기관간 협의 사항으로 결합률을 높이기 위한 목적 등 필요한 경우 복수로 생성할 수 있음(정보집합물 결합 신청시 결합 방식에 대한 구체적인 내용을 추가로 기재)
- 데이터전문기관별로 가능한 결합 방식이 상이할 수 있으므로, 정보집합물 결합을 의뢰하려는 데이터전문기관과 사전 협의 필요

Q13. 정보집합물 결합시 주민등록번호를 사용할 수 있는지?

A

- 주민등록번호는 「개인정보 보호법」 제24조의2(주민등록번호 처리의 제한)에 따라 결합키로 활용 불가

Q14. 결합전 결합 대상 정보집합물의 가명처리는 식별자만 제거해도 되는지?

A

- 식별자뿐만 아니라 개인식별가능정보도 적절히 처리되지 않을 경우 개인이 재식별될 수 있기 때문에, 결합 대상 정보집합물 내에서 개인이 식별되지 않도록 범주화, 라운딩, 상·하단 코딩 등을 적절히 활용하는 등 안내서에 따라 적절하게 가명처리해야 함(※ 「신용정보법」 시행령 제14조의2제3항제1호)

Q15. 이용기관이 다수인 경우, 결합정보를 다르게 구성하여 반출하는 것도 가능한지?

A

- 가능하나, 데이터전문기관별로 차이가 있을 수 있으므로 정보집합물 결합을 의뢰하려는 데이터전문기관과 사전 협의 필요

Q16. 제공받은 데이터를 가명처리 후 데이터전문기관을 통해 결합하는 것도 가능한지?

A

- 가능하나, 원 제공자와 체결한 계약 등에 제공받은 데이터의 가명처리 후 이용을 제한하는 내용이 없어야 함

Q17. 금융분야와 비금융분야간 정보집합물 결합시 신용정보법 또는 개인정보보호법 중 어떤 법에 따라 결합을 해야하는지?

A

- 결합의뢰기관에 신용정보회사등(법 17조 2항에 따른 상거래기업 및 법인 제외)이 포함될 경우에는 「신용정보법」에 따라 데이터전문기관을 통해 정보집합물 결합을 진행해야 함(※ 「신용정보법」 제17조의2제1항)
- 정보집합물 결합 이후에는 금융분야의 결합의뢰기관이나 이용기관은 「신용정보법」을, 비금융분야의 결합의뢰기관이나 이용기관은 「개인정보 보호법」에 따라 사후관리 수행

Q18. 결합 대상 정보집합물이 개인신용정보가 아닌 경우에도 결합의뢰기관에 금융기관이 포함되면 신용정보법상의 데이터전문기관을 이용해야 하는지?

A

- 「신용정보법」은 결합의뢰기관에 신용정보회사등의 포함 여부를 기준으로 「신용정보법」에 따른 정보집합물 결합 수행 여부를 판단하며, 결합 대상 정보집합물이 개인신용정보인지 여부는 판단기준이 아님

Q19. 결합률 사전통지(사전분석)을 데이터전문기관을 통하지 않고 관계회사끼리 자체적으로 할 수 있는지?

A

- 결합키 자체도 가명정보에 해당하고 결합률 확인도 정보집합물 결합에 해당하므로, 데이터전문기관을 통해서만 결합률 사전 확인 가능

Q20. 개인신용정보와 기업신용정보를 결합할 때에도 데이터전문기관을 통해야 하는지?

A

- 기업신용정보라 하더라도 개인신용정보와 연결될 때에는 결합정보가 개인신용정보이므로 데이터전문기관을 통해서 결합해야 함

3. 익명처리 적정성 평가

Q21. 집계성 데이터(부분총계)도 익명처리 적정성 평가 대상인지?

A

- 집계성 데이터는 통계자료로 보일 수는 있으나, 구성 칼럼이나 레코드, 부분총계를 나누는 기준의 구체성 등에 따라 외부 정보와의 연계 등을 통해 개인이 식별될 가능성이 존재
- 필요시 익명처리 적정성 평가를 통해 재식별 위험성 등을 검토 및 추가 익명처리를 한 후 해당 데이터를 이용할 것을 권고

Q22. 비금융기관도 데이터전문기관에 익명처리 적정성 평가를 신청할 수 있는지?

A

- 「신용정보법」상의 익명처리 적정성 평가는 신용정보회사등만 신청 가능
  (※ 「신용정보법」 제40조의2제3항)

Q23. 데이터전문기관을 통한 익명처리 적정성 평가를 받은 익명정보만 이용 목적에 제한이 없는 것인지?

A

- 데이터전문기관의 익명처리 적정성 평가를 거쳤는지 여부와는 상관 없이 익명정보는 이용 목적에 제한은 없음
- 신용정보회사등이 자체적으로 수행한 익명처리 적정성 평가의 경우 해당 데이터가 개인신용정보가 아니라는 법적 추정력이 부여되지 않으므로 신용정보회사등이 스스로 그 결과에 책임을 져야 하나 데이터전문기관을 통한 익명처리 적정성 평가의 경우 해당 데이터가 더 이상 개인신용정보가 아니라는 법적 추정력이 부여된다는 이점이 있음
  (※ 「신용정보법」 제40조의2제4항)

4. 법령 관련

Q24. 원본정보와 가명정보 취급 직원을 분리해서 정해야 하는데, 추가정보 담당자도 별도로 지정해야 하는지?

A

- 추가정보 담당자를 별도로 지정할 필요는 없으며 가명정보 취급자는 원본 및 추가정보에 접근하지 않아야 함

(※「신용정보업감독규정」 별표 8)

Q25. 결합의뢰기관인 동시에 이용기관일 경우 결합정보(가명정보)를 받으면, 결합 전 정보와 분리보관해야 하는지?

A

- 결합 전 데이터는 가명처리 여부와는 관계 없이 결합정보의 원본정보로 보아야 하므로, 결합목적으로 생성한 가명정보는 정보집합물 결합이 완료되면 그 이용목적을 달성한 것이므로 삭제하는 것이 바람직하며 부득이하게 보관하여야 할 경우에는 결합 전 데이터와 결합정보는 분리보관해야 함

Q26. 원본정보 취급자가 가명정보 생성한 이후, 원본정보 접근 권한은 회수하고 가명정보 처리자로 지정되는 것도 가능한지?

A

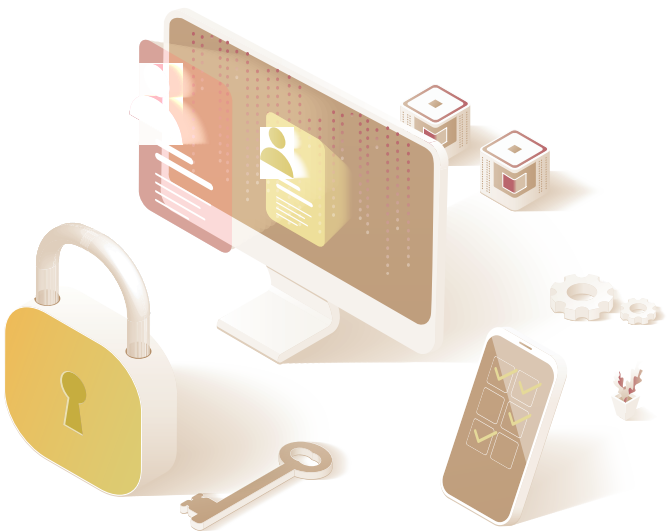
- 원본정보 접근권한과 가명정보 접근권한을 같은 사람에게 필요에 따라 자주 반복 부여하는 등 제도를 악용하는 것이 아닌 한 가능할 수 있지만(가명정보 처리자가 된 이후에는 원본정보 및 추가정보에 접근할 수 없어야 함), 권장하지 않음
- 부득이한 경우에는 관리책임자의 승인을 얻어 원본정보와 가명정보에 한시적으로 동시 접근 가능하도록 권한을 부여할 수 있으나 관련 기록을 보관하여야 함

(※「신용정보업감독규정」 별표8)

Q27. 제공 받은 결합정보(가명정보)를 제3자에게 다시 제공하는 것이 가능한지?

A

- 결합정보(가명정보)는 데이터전문기관에서 결합시 한정된 이용기관을 대상으로 적정성 평가 등이 이루어졌으므로 임의로 제3자에게 제공 불가능(※ 본 안내서 Ⅳ.정보집합물 결합-2.결합 절차-차.결합정보 활용 참고)하나, 그 결합정보를 분석한 결과 등은 제공 가능



부록10 신용정보법 시행령 및 감독규정 개정 주요내용

◎ '22년내 신용정보법 시행령 및 감독규정 개정 및 시행이 예정되어 있어 가명 · 익명처리에 참고할 수 있도록 개정 주요내용 및 관련 절차 · 서식을 공개

◎ 본 안내서는 개정 시행이후 관련 내용을 추가 반영할 예정으로, 최신 버전의 안내서는 금융위원회 홈페이지(www.fsc.go.kr) 또는 금융감독원 홈페이지(ww.fss.or.kr) 참고

1. 데이터 이용기관의 데이터 결합신청 허용(영 §14의2, 규정 §15의2)

• **(현행)** 現 신정법령에서는 자기가 보유한 데이터가 아닌 타 기관들이 보유한 데이터만을 결합 · 이용하려는 경우에도,

– 데이터 결합 신청 등 결합을 위한 행정 및 지원업무 등을 모두 데이터를 보유한 기관이 하도록 하고 있어*, 데이터 미보유기관이 타 기관 데이터를 결합 · 활용하는데 애로

* 데이터 보유기관이 전문기관에서 결합이 완료된 데이터를 받아 이용기관에 전달

• **(개선)** 결합할 데이터를 이용하려는 기관(데이터 이용기관)의 데이터 결합 신청* 등을 할 수 있도록 허용

* 데이터 이용기관은 데이터 보유기관과 데이터 제공협의가 완료된 이후 결합신청

– 데이터 보유기관은 결합할 데이터의 가명처리 및 전문기관에 결합할 데이터 전송만 담당하고, 이외 절차는 이용기관이 수행

※ 개보법의 경우 데이터 이용기관의 데이터 결합 신청 및 참여 旣 허용

2. 샘플링 결합* 절차 도입(영 §14의2, 규정 §15의2)

* 대량의 데이터중 일부를 추출하여 결합·활용하는 방식(예: 全 국민의 노후대비 실태 연구시 국민연금, 은행 등 각 기관에서 全 국민의 5%만 추출하여 결합·활용)

• **(현행)** 現 결합제도에서는 샘플링하여 결합하는 것이 제한됨*

* 각 기관이 동일한 샘플을 추출하여야 하므로 샘플링된 결합키를 상대기관에 제공하여야 하나 결합키는 개인정보로 정보주체 동의없이 제3자 제공 불가

– 결합데이터의 일부만 샘플링해서 활용하려는 경우에도 전체 데이터를 전문기관에 제공·결합할 필요* → 비효율적인 측면

* 예) A은행과 B카드사가 중복되는 고객중 5%만 샘플링하여 결합·활용하려는 경우에도 A은행과 B카드사의 전체 고객정보를 결합한 후 샘플링하여야 함

• **(개선)** 샘플링하여 데이터를 결합하는 '샘플링 결합' 절차 도입

– 샘플링 결합 선택시 샘플링된 데이터만 데이터 전문기관에 전송하여 결합할 수 있어 효율적 결합 수행 가능

* ① 모든 결합참여기관이 결합키만 데이터전문기관에 송부 → ② 결합키만 결합후 데이터전문기관이 일부 결합키를 샘플링 → ③ 샘플링된 결합키를 각 결합기관에 전달 → ④ 각 참여기관은 샘플링된 키에 해당하는 데이터만 전문기관에 보내 결합

3. 데이터 자가결합 허용요건 확대(규정 §15의2)

• **(현행)** 데이터전문기관이 자가결합[i]할 경우 이해상충 우려[ii]가 있어 이해상충 가능성이 없는 경우에만 허용중

* ⅰ) 데이터전문기관이 자신이 보유한 데이터와 제3자의 데이터를 결합

ⅱ) 데이터전문기관이 결합된 데이터의 가명처리 적정성을 평가하여 결합의뢰기관에 제공 → 전문기관이 결합의뢰기관인 경우 스스로 평가하는 이해상충 발생

– 이해상충 가능성이 없는 경우를 결합데이터의 제3자 제공(개방)으로 매우 제한적으로 규정 → 데이터 결합 활성화 저해 요인

※ 데이터전문기관 역할 : ①금융회사와 제3자의 데이터 결합, ②결합데이터의 가명처리 적정성 평가, ③익명데이터의 익명처리 적정성 평가 등

• **(개선)** 이해상충 가능성이 없는 경우에 적정성 평가를 타 전문기관이 수행하는 경우를 추가하는 등 합리적으로 확대

4. 데이터 전문기관 지정 유효기간 신설(규정 §28의3)

• **(현행)** 전문기관 지정 유효기간이 없어 전문기관으로 지정받은 이후 전문기관으로서의 공적인 역할을 소홀히 할 우려

* 현재 고의·중대과실로 업무를 부실하게 수행하는 경우에만 전문기관 지정취소 가능

• **(개선)** 전문기관 지정이후에도 전문기관의 충실한 업무수행 유도 등을 위해 지정 유효기간(3년) 부여 → 매 3년마다 재심사

※ 개보법은 시행령(§29의2④)에서 전문기관 지정 유효기간을 3년으로 旣 규정

5. 데이터전문기관 지정 요건 합리화(규정 별표7)

• **(현행)** 현행 데이터전문기관 지정 요건은 민간기업이나 비영리법인 등을 상정하고 구성되어 있어,

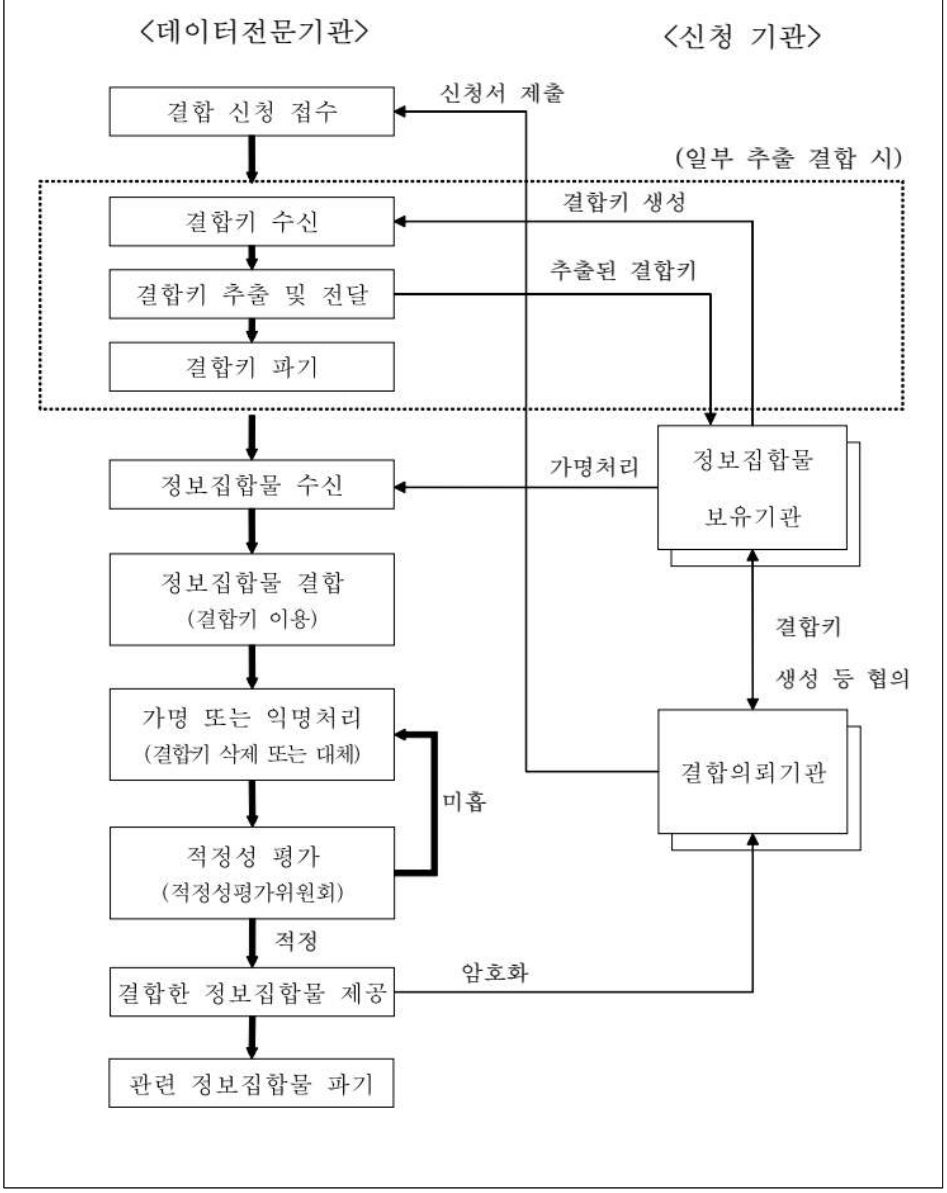
– 국가기관에 대해 데이터전문기관 지정을 심사할 경우 적용이 어렵거나 불필요한 지정요건*도 적용되는 상황

* 임원 적격성 요건, 재정능력(순자산 대비 부채총액 비율) 요건 등

• **(개선)** 임원 적격성 요건, 재정능력 등은 국가기관에 미적용

〈 개정 결합 절차 및 신청서 양식 〉

[별표 2의4] 정보집합물 결합 관련 절차 (제15조의2제6항 관련)



[별지 제8호의2 서식] 정보집합물 결합신청서(제15조의2제1항 관련)

정보집합물 결합 신청서

<table>
<tr><td>접수번호</td><td colspan="2"></td><td>접수일</td><td></td></tr>
<tr><td rowspan="3">결합의뢰
기관명</td><td>기관명</td><td></td><td>담당자(성명,직함)</td><td></td></tr>
<tr><td>담당부서</td><td></td><td>전화번호</td><td></td></tr>
<tr><td>소재지</td><td></td><td>이메일 주소</td><td></td></tr>
<tr><td rowspan="3">정보집합물
보유기관명
(복수기재 가능)</td><td>기관명</td><td colspan="3"></td></tr>
<tr><td>담당부서</td><td colspan="3"></td></tr>
<tr><td>소재지</td><td colspan="3"></td></tr>
<tr><td colspan="2">결합목적</td><td colspan="3"></td></tr>
<tr><td colspan="2">정보집합물
주요내용 요약</td><td colspan="3"></td></tr>
<tr><td colspan="2" rowspan="3">결합 데이터
제공형태</td><td rowspan="2">☐ 가명정보</td><td>이용목적</td><td>☐ 통계작성 (상업적 목적 포함)
☐ 연구 (산업적 연구 포함)
☐ 공익적 기록보존 등</td></tr>
<tr><td>결합키</td><td>☐ 삭제
☐ 대체</td></tr>
<tr><td colspan="3">☐ 익명정보</td></tr>
<tr><td colspan="2">기타사항</td><td colspan="3"></td></tr>
</table>

「신용정보의 이용 및 보호에 관한 법률」 제17조의2제1항에 따라 위와 같이 신청합니다.

년 월 일

신청인 (서명 또는 인)

(전문기관명)장 귀하

첨부서류	정보집합물의 데이터 명세서, 정보집합물 보유기관의 정보집합물 제공 사실 확인서류 등

참고문헌

- 개인정보보호위원회, 『가명정보 처리 가이드라인』, 2021.10.
- 정부부처 합동, 『개인정보 비식별 조치 가이드라인』, 2016.6.
- 과학기술정보통신부 · 한국정보화진흥원, 『2019 개인정보 비식별 기술 가이드라인』, 2019.12.
- 한국금융연수원,「한국신용정보원 가명처리 · 익명처리 전문가 양성」(연수자료), 2020.5.
- 금융보안원, 「금융부문 암호기술 활용 가이드」 (AGR-VII-2019-②-84), 2019.1.
- ISO/IEC, "Privacy enhancing data de-identification terminology and classification of techniques", ISO/IEC 20889, First edition, 2018.11.
- ISO/IEC, "Health informatics — Pseudonymization", ISO/IEC 25237, 2017.1.
- ENISA, "Recommendations on shaping technology according to GDPR provisions: An overview on data pseudonymisation", 2018.11.
- Simson L. Garfinkel , "De-Identification of Personal Information", NIST, NISTIR 8053, 2015.10.

금융분야

가명·익명처리 안내서

2022년 1월 발행

발행처 : 금융위원회, 금융감독원

본 안내서는 2022년 1월 기준으로 작성되었습니다.
최신 안내서는 금융위원회 또는 금융감독원
홈페이지에서 확인하시기 바랍니다.


금융위원회
금융감독원
FINANCIAL SUPERVISORY SERVICE

금융분야

가명·익명처리 안내서

금융위원회

금융감독원
FINANCIAL SUPERVISORY SERVICE