교육분야 가명·익명정보 처리 가이드라인

2022. 7.

교육부 Ministry of Education

개인정보보호위원회

교육분야 가명·익명정보 처리 가이드라인

가이드라인 활용 안내

<개요>
본 가이드라인은 교육분야 개인정보를 가명정보 및 익명정보로 처리하는 절차와 방법에 대한 내용을 제공하는 자료로 다음 사항을 참고하여 활용하시기 바랍니다.

1. 가이드라인 내용의 기본방향은 개인정보보호 관련 법령을 준수하여 학생, 학부모, 교직원 등 정보주체의 권리보호 및 개인정보처리자의 책임성 강화를 목적으로 합니다.

2. 본 가이드라인은 교육 분야의 특성을 고려한 최소한의 가명·익명 처리 기준을 안내하고 있습니다.

3. 가명·익명 처리 업무에 본 가이드라인을 활용하시기 바라며, 향후 법령의 변경 등에 따라 내용은 수정· 보완될 수 있습니다.

4. 본 가이드라인은 2022년 7월 기준으로 작성되었습니다. 항상 최신의 가이드라인은 교육부 개인정보보호 포털(자료실→참고자료)에서 확인하시기 바랍니다.

CONTENTS

Chapter

I

가이드라인 개요

Ⅰ 가이드라인 개요

1 배경 및 목적

- 「개인정보 보호법」 시행('20.8.5.)에 따라 가명정보, 익명정보를 활용하여 통계작성, 과학적 연구 및 공익적 기록보존 등에 다양하게 활용할 수 있는 기반 마련

- 데이터 3법 개정·시행과 더불어 「데이터기반행정법」과 「공공데이터법」 시행('20.12.10.)으로 공공기관이 수행해야 할 데이터 처리 및 교육정보 활용을 위한 수요 증가가 예상되어 교육분야의 특수성을 고려한 안전한 가명·익명처리 체계 마련

- 이에 본 가이드라인은 교육분야의 가명·익명정보를 처리하는 과정에서 발생할 수 있는 개인정보 오·남용을 방지하고 안전한 가명·익명정보 처리 방안을 제시하여 교육정보 활용을 통한 효율적 교육정책 수립뿐만 아니라 교육기관의 안전한 행정기반 데이터 처리 및 정보주체의 권익을 보호할 수 있는 안전성을 지원하고자 함

관 련 법 령

- 개인정보 보호법 제2조 및 제28조의2부터 제28조의6
  * 가명정보의 처리, 결합제한, 안전조치의무, 금지의무, 과징금 부과 등
- 개인정보 보호법 시행령 제29조의2부터 제29조의6
- 가명정보의 결합 및 반출 등에 관한 고시
- 가명정보 처리 가이드라인(개인정보보호위원회, '22.4.)

2 적용 범위

- **(우선순위)** 교육 분야의 개인정보 가명·익명처리 및 결합 등에 관해서는 동 가이드라인을 우선 적용

※ 동 가이드라인에서 별도로 정하지 않은 사항은 개인정보보호위원회 『가명정보 처리 가이드라인』 준용

- **(적용대상)** 교육행정기관*, 학교** 및 교육부장관의 지도감독을 받는 공공기관 및 단체***(이하 "각급기관"이라 한다.)의 개인정보처리자와 각급기관으로부터 정보를 제공받은 자

* 교육부 및 그 소속 기관과 특별시·광역시·특별자치시·도 또는 특별자치도의 교육 관서(교육공무원법 제2조제4항)

** 유아교육법 제2조제2호에 따라 설립된 유치원 및 초·중등교육법 제2조·고등교육법 제2조에 따라 설립된 각급학교

*** 각급기관으로부터 정보시스템 구축·운영을 위탁받은 기관 및 단체 포함

- **(적용범위)** 본 가이드라인은 다음의 내용을 참고하여 적용범위를 고려

• 가명처리 : 개인정보 보호법 제28조의2(가명정보의 처리 등)에 근거하여 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 가명처리에 적용

※ 개인정보 보호법 제15조 제3항 및 제17조 제4항 등에 근거한 가명처리*는 본 가이드라인의 적용범위가 아니나 주요 내용은 참고할 수 있음

* 시행령 제14조의2 제1항에 따라 당초 수집 목적과 합리적으로 관련된 범위 내에서 안전성 확보조치에 필요한 조치로 가명처리를 하는 경우를 의미하며 이 경우에는 법령에서 요구하는 사항은 준수하여야 함

• 익명처리 : 개인정보 보호법 제58조의2(적용 제외)에 근거하여 당사자가 누구인지 알아볼 수 없는 형태로 제공하는 경우에 적용

※ 초·중등교육법 제30조의6(학생 관련 자료 제공의 제한) 제1항 제3호 '통계작성 및 학술연구 등의 목적을 위한 것으로서 자료의 당사자가 누구인지 알아볼 수 없는 형태로 제공하는 경우'에서 제공되는 정보는 익명정보를 의미하며 교육기관은 익명처리를 적용해야 함

※ 교육관련 법령에서 '누구인지 알아볼 수 없는 형태'는 익명정보를 의미

3 용어 정리

개인정보 : 살아있는 개인에 관한 정보로서 다음의 정보를 포함

가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보

나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 함

다. 가목 또는 나목을 가명처리함으로써 원래의 상태로 복원하기 위한 추가정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보

※ 개인정보에 대한 판단기준은 개인정보처리자가 보유한 정보 또는 접근 가능한 권한 등 개인정보 처리상황에 따라 다르게 판단되어야 함

개인식별정보(식별자)

- 고유식별정보, 이메일주소, 휴대전화번호 등과 같이 그 자체로 특정 개인을 직접 식별하는 용도로 사용하는 정보

개인식별가능정보(준식별자 또는 간접식별자)

- 연령, 성별, 거주 지역, 국적 등과 같이 해당 정보만으로는 직접적으로 특정 개인을 식별할 수 없지만, 다른 정보와 결합하여 특정 개인을 전부 또는 일부 식별할 수 있는 정보

※ 개인식별가능정보는 개인 식별 가능성이 높고 낮음에 따라 가명처리 및 익명처리 수준 등을 달리할 수 있으며, 해당 속성의 개인 식별 가능성 여부는 구체적인 사례에 따라 달리 판단 해야함

개인정보처리자

- 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등

가명처리

- 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것

가명정보

- 개인정보를 가명처리 함으로써 원래의 상태로 복원하기 위한 추가정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보

※ 가명정보도 개인정보의 범주에 포함

가명정보처리자

- 업무를 목적으로 개인정보를 가명처리하여 활용 또는 제공하는 공공기관, 법인, 단체 및 개인 등

가명정보취급자

- 가명정보를 처리하는 개인정보처리자의 지휘·감독을 받아 가명정보를 처리하는 임직원, 파견근로자, 시간제근로자 등

추가정보

- 개인정보의 전부 또는 일부를 대체하는 가명처리 과정에서 생성 또는 사용된 정보로서 특정 개인을 알아보기 위하여 사용·결합될 수 있는 정보(알고리즘, 매핑테이블 정보, 가명처리에 사용된 개인정보 등)

※ 가명처리 과정에서 생성·사용된 정보에 한정된다는 점에서 '다른 정보'와 구분됨

특이정보

- 다른 데이터와 확연히 구분되거나 비정상적으로 데이터의 분포를 벗어나 측정이 되는 값으로서, 개인정보 식별과 관련하여 특정 개인의 식별 가능성이 매우 높은 정보

다른 정보

- 추가정보에 포함되지 않으면서 가명정보취급자가 가명정보의 처리 시점에 활용할 수 있거나 재식별에 이용될 가능성이 있는 정보

※ 가명정보처리자, 가명정보취급자가 보유하고 있거나 합리적으로 입수 가능한 정보에 한함

가명정보처리시스템

- 개인정보를 가명처리하거나 가명정보를 처리할 수 있도록 체계적으로 구성한 시스템

익명정보

- 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보

익명처리

- 개인정보의 전부 또는 일부를 데이터 값 삭제, 가명처리, 총계처리, 범주화 등 다양한 기술을 적용함으로써 더 이상 특정 개인을 알아볼 수 없도록 익명정보로 처리하는 것

익명정보처리자

- 업무를 목적으로 개인정보를 익명처리하여 활용 또는 제공하는 공공기관, 법인, 단체 및 개인 등

적합성 검토

- 가명정보를 처리(이용)하는 목적 및 관련 사항들이 적합한 지 여부를 판단하는 절차

적정성 검토

- 본 가이드라인에서 제시하고 있는 절차를 기반으로 사전에 정의한 처리 기준에 따라 적절히 가명·익명처리 되었는지 확인하는 절차

재식별

- 특정 개인을 알아볼 수 없도록 처리한 가명·익명정보에서 특정 개인을 알아보는 것

개인정보파일

- 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물

결합키

- 결합 대상 가명정보의 일부로서 해당 정보만으로는 특정 개인을 알아볼 수 없으나 다른 결합대상정보와 구별할 수 있도록 조치한 정보로서, 서로 다른 가명정보를 결합할 때 매개체로 이용하는 값

결합키연계정보

- 결합키가 동일한 정보에 관한 가명정보를 결합할 수 있도록 서로 다른 결합신청자의 결합키를 연계한 정보

결합대상정보

- 결합신청자가 결합을 위해 결합전문기관에 제공하는 가명정보에서 결합키를 제외한 정보

결합정보

- 결합전문기관을 통해 결합대상정보를 결합하여 생성된 정보

반출정보

- 결합전문기관에서 결합된 결합정보 중 결합전문기관의 심사를 통해 반출된 정보

결합신청자

- 가명정보의 결합을 신청하는 개인정보처리자 등

※ 가명정보를 제공하거나 이용하는 자(공공기관, 법인, 단체, 개인 등)

결합전문기관

- 개인정보 보호법 제28조의3제1항에 따라 서로 다른 개인정보처리자 간의 가명정보 결합을 수행하기 위해 개인정보보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관

결합키관리기관

- 개인정보 보호법 시행령 제29조의3제2항에 따라 결합키연계정보를 생성하여 결합전문기관에 제공하는 등 가명정보의 안전한 결합을 지원하는 업무를 하는 한국인터넷진흥원 또는 개인정보보호위원회가 지정하여 고시하는 기관

동질집합

- 같은 속성자 값들로 가명·익명처리된 레코드들의 모임으로 '동일 속성자 값 집합(Equivalent Class)'

Chapter

II

가명처리 및 가명정보 처리

Ⅱ 가명처리 및 가명정보 처리

1 개요

가명정보는 통계작성, 과학적 연구, 공익적 기록보존 등의 목적으로 정보주체의 동의 없이 처리 가능

가명처리 목적

○ 통계작성

- 집단적 현상이나 수집된 자료의 내용에 관한 수량적인 정보를 작성하는 행위를 말함

※ 직접(1:1) 마케팅 등을 위하여 특정 개인을 식별할 수 있는 형태의 통계는 해당하지 않음

▸ (예시) 대학이 학생들의 취업 활동 지원(직업군 및 교육과정 추천)을 위하여 가명 처리된 졸업생들의 학습이력 분석과 취업기관 및 유형들에 대한 매칭 통계를 작성하는 경우

○ 과학적 연구

- 기술 개발, 실증, 기초연구, 응용연구, 민간투자연구 등 과학적 방법을 적용하는 연구를 말함

※ 자연과학적 연구뿐만 아니라 과학적 방법을 적용하는 연구, 학생 보건 분야에서 공익을 위해 시행되는 연구 등을 포함

▸ (예시) 교육부가 학생의 학습 및 미래 보장 서비스 구축 운영을 위해 학생생활기록부, 건강기록부, 출결 정보 등을 심층 분석하여 위기징후* 탐지 알고리즘 연구를 수행하려는 경우

* 중도 학업 포기, 학교폭력 등

공익적 기록보존

- 공공의 이익을 위하여 지속적으로 열람할 가치가 있는 기록정보를 보존하는 것을 말함

※ 공공기관이 처리하는 경우에만 공익적 목적이 인정되는 것은 아니며, 민간기업, 단체 등이 일반적인 공익을 위하여 기록을 보존하는 경우도 공익적 기록보존 목적이 인정됨

▸ (예시) 학내 연구소가 현대사 연구 과정에서 수집한 개인정보 중에서 사료 가치가 있는 인물에 관한 정보를 기록하여 보관하는 경우

가명처리와 가명정보의 처리

"가명처리"는 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하여 가명정보를 생성하는 과정을 의미하며

"가명정보 처리"는 가명처리를 통해 생성된 가명정보를 이용·제공 등 처리(활용)하는 행위를 말함

가명처리 원칙

가명처리 대상은 법률에서 허용한 목적 내에서 개인정보를 정보 주체의 추가적인 동의 없이 수집 목적 외로 이용 가능

▸ 고유식별정보는 직접 식별자에 해당하므로 고유식별정보가 남아있거나 역추적이 가능하도록 해서는 안됨(고유식별정보 중에서 주민등록번호는 가명처리 대상 선정 자체가 불가)

개인식별정보(식별자)는 삭제하여야 하나, 결합 등 데이터 이용목적 상 필요한 경우 안전한 방식으로 대체값을 생성하여 개인식별정보를 대체

개인정보를 가명처리하는 과정에서 발생한 추가정보 삭제

- 다만, 불가피한 경우* 추가정보는 분리보관 등 안전성 확보조치를 취하여 보관 가능

* 시계열 분석 등을 위한 일련번호 및 결합키 생성 등

※ 추가정보를 삭제한 경우 가명정보 관리대장에 삭제 여부를 작성해야 함

- 가명처리는 개인정보 보유부서 또는 총괄부서*를 지정하여 처리

  * 개인정보처리자는 가명처리 관련 업무의 총괄·관리 및 의사결정을 위한 총괄부서(또는 담당자) 지정 가능

  ※ 내부결합, 익명처리 등도 위와 준하여 처리

- 가명처리 관련 업무 및 취급 권한 분리

  • 가명처리를 수행하는 자와 가명정보의 적정성을 검토하는 자*, 가명정보취급자(활용 등)는 관리적·기술적으로 권한 분리

  * 추가정보의 내용을 알고 있는 자가 가명정보의 검토를 수행하거나 취급(활용)하는 경우, 처리하는 과정에서 특정 개인을 알아볼 우려가 있음

  • 취급권한을 분리할 수 없는 불가피한 사유가 있을 경우 보완통제 대책을 수립하여 관리자의 승인 하에 제한적으로 취급 가능

  ※ 해당 부서 소유 개인정보를 가명처리하여 해당 부서에서만 사용하는 등 가명정보를 취급할 자를 추가로 둘 여력이 없거나 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 취급권한 부여와 관련 기록을 보관 하는 등 예외적으로 보안대책을 수립한 후 허용

  • 가명정보를 제공받는 제3자는 해당 가명처리 과정에 참여 불가

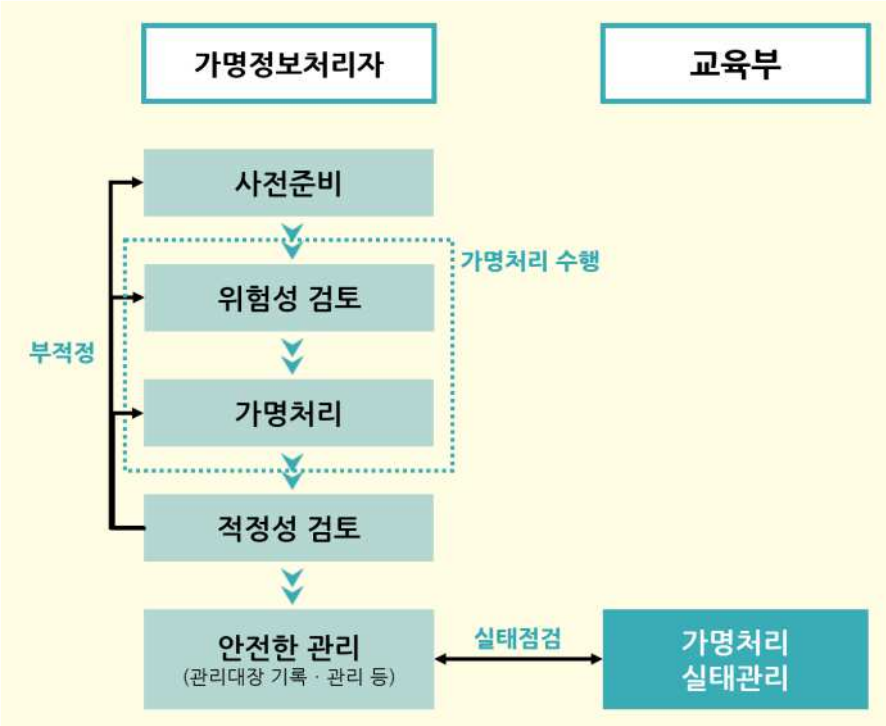
  ※ 단, 상위 관리·감독 기관인 경우 취급자 권한 분리 등을 통해 가명처리 지원 가능

- 안전한 가명처리 방법을 적용하여 가명정보로 변환

- 개인정보처리자는 가명정보 처리업무를 외부에 위탁하는 경우, 위탁 계약서 등에 재식별 금지 및 안전성 확보조치 관련 내용들을 포함하여 진행

- 개인정보처리자는 가명정보를 처리하는 자 등에 대해 연 1회 이상 가명처리 관련 교육을 실시하거나 관련 교육 및 기술 세미나 등에 참석할 수 있도록 조치

가명처리 절차 개념도



<그림 1> 가명처리 절차

- **(사전준비)** 가명처리 목적을 명확히 정의하고 가명처리 대상 개인 정보를 선정
- **(위험성 검토)** 처리대상 개인정보의 식별 위험성을 검토하는 것으로 데이터 자체 및 처리환경에 대한 식별 위험성을 검토
- **(가명처리)** 식별 위험성 검토 결과에 따라 가명처리 방법과 수준을 정의하고 수준에 맞도록 가명처리 기법을 활용하여 개인정보를 가명처리
- **(적정성 검토)** 목적 달성 가능성, 가명처리 수준 등에 맞는 가명처리가 되었는지 여부를 확인하고 가명정보 내 개인정보 재식별 여부 및 재식별 가능성을 검토

※ “부적정” 판단 시 판단 결과에 따라 해당 단계로 이동

- **(안전한 관리)** 가명처리된 가명정보와 추가정보에 대해 안전성 확보조치를 수행하고, 재식별 모니터링 및 재식별사고 발생 등에 관한 대책 수립 및 이행

- **(가명처리 실태관리)** 가명처리 현황 및 안전성 확보 조치 등에 대해 조사·점검 등 실시

가명처리 예시

[원본 정보]

성명	연락처	성별	생년월일	혈액형		전공	학위
				ABO	RH		
김영희	090-1234-5678	여	19650512	A	Rh+	법학	박사
강순희	090-8525-4564	남	19671212	B	Rh+	컴퓨터	학사
최복례	090-8546-5456	여	19681015	O	Rh+	건축	학사
홍길동	090-5524-1325	남	19920721	AB	Rh-	보안	학사
이홍준	090-6974-1235	남	19930423	AB	Rh+	교육	학사
김신우	090-3456-7890	남	19940925	O	Rh+	음악	학사
…	…	…	…	…	…	…	…

[표 1] 개인정보 원본 예시

- 성별/혈액형별 나이와 전공 및 학위에 대한 상관관계 연구 목적으로 가명처리를 하는 경우 '성명', '연락처'는 직접적으로 개인 식별이 가능
- '성별', '생년월일'은 다른 정보와 조합하여 개인을 식별할 가능성이 높고 '혈액형'에서 Rh-의 경우 희귀 혈액형 유형으로 개인이 식별될 가능성이 매우 높음.
- '전공', '학위'는 다른 정보와 결합하여 개인이 식별될 가능성이 있으나 비교적 낮음

[가명처리]

- '성명', '연락처'는 특정 개인 식별이 가능하므로 삭제 처리를 하되, 데이터의 이용 목적상 개인을 특정할 필요가 있는 경우나 결합이 필요한 경우 결합키의 입력값으로 활용
  ☞ 가명처리 기법인 해시함수(SHA-256 이상)와 솔트값(salt)을 적용하여 결합키 생성
- '성별', '생년월일'은 다른 정보와 조합하여 개인을 식별할 가능성이 비교적 높고 '혈액형'에서 Rh-의 경우 희귀 혈액형 유형으로 개인이 식별될 가능성이 매우 높음. 따라서 혈액형에서 Rh-의 경우 특이정보로 판단하여 해당 레코드를 삭제 처리하고 생년월일은 출생년도로 범주화. 다만, 전체 데이터에서 목적에 따라 검증하여 특정인이 식별되는 경우 범주화를 연령대로 확대하거나 특정 레코드 삭제 등 수행
- '전공', '학위'는 다른 정보와 조합하여 개인이 식별될 가능성이 있으나 특이 전공 등이 존재하는 지 확인하여 개인 식별 가능성이 낮은 경우 별도 가명조치 없이 그대로 활용

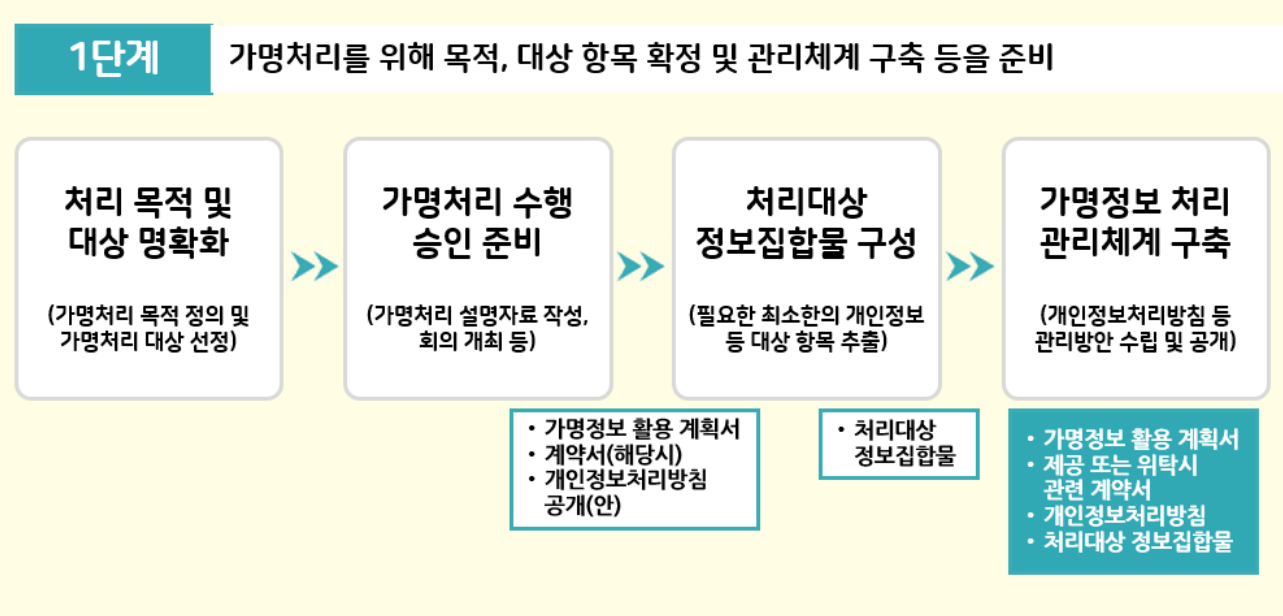
성명	연락처	성별	생년월일	혈액형		전공	학위
				ABO	RH		
		여	1965	A	Rh+	법학	박사
		남	1967	B	Rh+	컴퓨터	학사
		여	1968	O	Rh+	건축	학사
		남	1993	AB	Rh+	교육	학사
		남	1994	O	Rh+	음악	학사
		…	…	…	…	…	…

[표 2] 가명처리된 정보 예시

※ 가명정보 처리 목적이 월별 통계정보를 구하는 경우 월을 제외한 나머지 데이터를 삭제하는 기법의 가명처리 수행(19940925 → 09) 등 목적 고려 필요

2 가명처리 세부 절차

2-1 사전준비(1단계)



<그림 2> 가명처리 사전준비 단계 세부 절차

- **(처리 목적 및 대상 명확화)** 가명처리 목적*을 명확히 정의하고 가명처리 대상 개인정보(개인정보파일, DB, 테이블 등) 선정

  * 통계작성, 과학적 연구(산업적 연구 포함), 공익적 기록보존 목적 등

- **(가명처리 수행 승인 준비)** 가명처리 관련 이해관계자 회의 개최 및 계획 수립 후 기관장 또는 개인정보 보호책임자* 등의 내부의사결정에 따라 승인 후 가명처리 수행을 준비

  * 개인정보처리자의 개인정보 처리에 관한 업무 총괄 책임자

☞ **주요 처리 사항**

- 기관 외부에 가명정보를 제공하는 경우 사업계획 준비 단계에서 이용목적 및 방법, 재식별 금지, 재식별 위험관리, 가명정보의 안전성 확보 조치, 목적외 사용 제한, 파기 관련 등의 내용을 포함한 계약서(안) 마련

  ※ 제Ⅱ편 > 3. 가명정보 안전조치 > 관리적 보호조치, (제3자 제공 시 계약 주의사항) 관련 계약서 포함 사항 참조

  ※ 타 기관과 가명정보의 결합을 위해 제공하는 경우도 동일
- 가명정보 처리에 관한 개인정보 처리방침 공개(안)을 작성하고 승인 후 개인정보 처리방침에 공개
- 가명처리 과정에서 발생할 수 있는 개인 식별 위험성을 확인하고 해결방안을 포함한 자료 첨부
- 가명정보를 이용하는 기관의 개인정보 보호수준에 따른 위험성을 점검하고 해당 자료 첨부

- **(처리 대상 정보집합물 구성)** 가명처리 목적 달성을 위해 필요한 최소한의 항목을 추출하여 가명처리 대상 정보집합물(데이터) 구성

- **(가명정보 처리 관리체계 구축)** 가명정보를 안전하게 처리할 수 있는 관리방안을 수립하고 가명정보 및 추가정보 등에 대한 관리체계를 구축

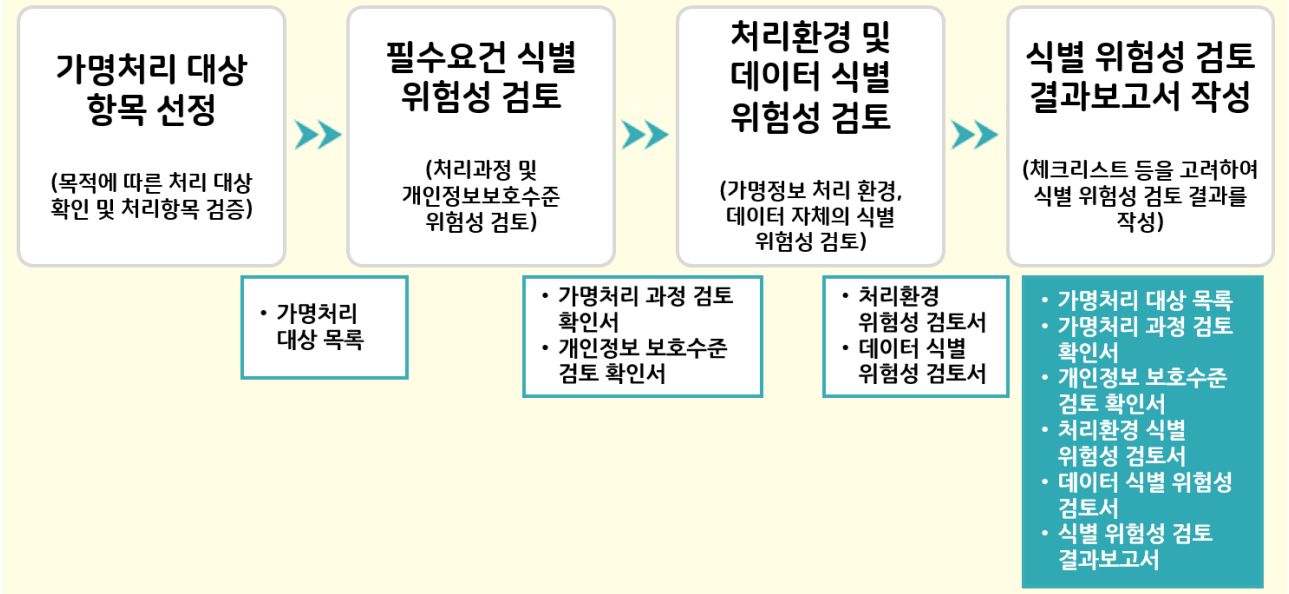
  ※ 안전성 확보조치 및 접근관리 방안 등 수립, 가명정보취급자 지정 등

주요 산출물

- 가명정보 활용 계획서
  - 가명정보 이용 위탁 시에는 위수탁계약서(안) 포함
  - 제3자 제공 시에는 제공 관련 계약서(안) 포함
- 개인정보 처리방침 공개(안)
- 처리대상 정보집합물(개인정보 데이터)

2-2 위험성 검토(2단계)

2단계 처리 과정, 보호수준, 처리 환경 및 데이터 식별 등에 대한 위험성을 검토



<그림 3> 위험성 검토 단계 세부 절차

가명처리 대상 항목 선정

○ 사업계획서 등을 통해 정보집합물에서 처리대상 및 대상별 특성을 확인하고 가명처리에 필요한 최소한의 항목을 추출

▸ 정보집합물 항목 선정 (예시)
- 이름, 휴대폰 번호, 성별, 이메일, **주소***, 재학 학교명, 학년/반/번호

▸ 가명처리 목적 (예시) : 학교별 재학생의 성별 및 지역분포 통계
- 성별, **시군구 주소**, 재학 학교명

* 최소한의 항목 추출 원칙에 따라 주소는 전체 주소가 아닌 시군구 주소만 추출

※ 분석 목적과 상관없는 개인정보 및 기타 정보는 대상 선정에서 제외

※ 본 단계는 사전준비 단계에서 추출한 정보집합물을 중복 검증하는 단계를 의미하여 정보집합물을 추출한 부서와 가명처리 업무를 수행하는 부서가 같은 경우 생략이 가능함

○ 선정된 대상에 대해 아래와 같이 위험성 검토 항목을 분류하고 필수 요건, 처리 환경, 데이터에 대한 식별 위험성을 검토

구분		주요 내용
항목	세부 항목	
필수 요건	가명처리 과정	가명처리과정에서 발생하는 위험성 검토
	이용기관의 보호수준	가명정보를 처리하게 되는 기관의 개인정보 안전성 확보조치 관련 법적 준수사항 검토
처리 환경	가명정보 처리 장소 및 형태	가명처리 장소 및 형태에 따른 위험성 검토
	다른 정보	다른 정보 보유, 접근 및 경험 등에 따른 위험성 검토
	이용기관의 신뢰도	가명정보를 처리하게 되는 기관의 신뢰수준에 따른 위험성 검토
	재식별 영향도	개인정보 재식별에 따른 영향도의 위험성 검토
	우연한 재식별	우연한 재식별이 될 위험성 검토
데이터	개인정보 항목	개인정보 항목별 위험성 검토
	데이터 구성	정보집합물(데이터) 구성에 따른 위험성 검토
	데이터 분포	정보집합물(데이터) 분포에 따른 위험성 검토

[표 3] 위험성 검토 분류 항목 예시

필수 요건 위험성 검토

○ 가명처리 과정에서 발생할 수 있는 위험성을 판단하고 검증

- 계획서*에 제출한 내용을 통해 개인정보를 가명정보로 가명처리하는 일련의 과정에서 발생할 수 있는 위험성 검증

  * 가명정보 처리 계획서를 수립할 때 가명처리 하는 과정에서 발생하는 위험성 검토 내용을 포함하여야 함

○ 이용기관의 '개인정보 보호수준'* 관련 위험성을 판단하고 검증

- 처리업무를 위탁하거나 제3자에게 제공하는 경우 수탁자 및 제공받는 자의 개인정보 보호수준 관련 위험성을 판단·검증

  * 처리자나 또는 제공받는 자의 안전조치 수준은 법적 요구사항을 모두 만족해야 함 : 내부통제 위험성 등 안전성 확보조치에 관한 사항인 '가명정보의 안전한 관리를 위한 법제적 요구사항'(별지 8) 및 처리기관의 개인정보 보호수준 체크리스트(별지 10) 참조

처리 환경 및 데이터 식별 위험성 검토

○ 수용 가능한 목표 위험 수준(DoA, Degree of Assurance) 정의

- 개인정보처리자는 DoA*를 사전에 정의하거나 가명정보 처리 목적에 따라 정의하고, 정의한 DoA를 넘어서는 위험에 대해 보완조치 수행

* DoA 정의에 관한 세부 사항은 가명정보 처리 실무안내서(교육부 개인정보보호 포털 참고자료) 참조

[처리 환경 식별 위험성 검토]

○ 처리 장소 및 형태에 따른 위험성 검토

- 가명정보를 처리하는 장소 및 처리 형태에 따른 위험성 검토
- 처리 장소에 대한 검토는 접근통제 및 접근권한을 중심으로 검토 실시
  - ▸ 처리 장소 : 안전한 통제구역 → 통제구역 → 제한구역 → 일반구역 → 공개된 장소 순서로, 내부 부서 → 타 부서 → 외부 순서로 위험성이 증가한다.

구분	안전한 통제구역			통제구역			제한구역			일반구역			공개된 장소
조직 내 공간	내부 부서원 (1)	타 부서원 (2)	외부인 (5)	내부 부서원 (2)	타 부서원 (3)	외부인 (7)	내부 부서원 (3)	타 부서원 (5)	외부인 (8)	내부 부서원 (5)	타 부서원 (7)	외부인 (10)	동일 (20)
외부조직 공간	외부조직 내 인력 (8)			외부조직 내 인력 (10)			외부조직 내 인력 (13)			외부조직 내 인력 (15)			

[표 4] 처리 장소 및 형태별 위험성 (수치는 위험성의 크기 예시)

- 처리 형태에 대한 검토는 해당 처리 형태가 가지는 위험성을 얼마나 통제하느냐를 중심으로 검토 실시
  - ▸ 처리 형태 : 기관 자체 → 공동연구 → 위탁 → 제공 순서로, 교육기관 → 공공기관 → 민간기관 순서로 위험성 증가

다른 정보와의 결합을 통한 위험성 검토

- 가명정보처리자 또는 취급자가 원본정보, 추가정보, 다른 정보(경험 및 지식 포함)와의 결합을 통한 재식별의 위험성 검토
  - ▸ 기관 자체적으로 처리하는 경우 다른 정보뿐만 아니라 원본정보, 추가정보에 대한 접근통제 및 권한 등 위험성 검토
  - ▸ 위탁 및 제3자 제공의 경우 공개된 정보 및 다른 정보와의 결합을 통한 식별 위험성 검토

이용기관의 신뢰도 관련 위험성 검토

- 가명정보를 제3자에게 제공하는 경우 가명정보 활용 계획서(안)과 이용기관의 신뢰도를 참고하여 위험성 검토.
  - ▸ 개인정보 보호법 제66조에 따라 법 위반으로 공표사실에 해당하는 기관인지 여부 확인, 위탁 및 제3자 제공시 준수사항 확인 등

우연한 재식별 관련 위험성 검토

- 우연한 재식별이 발생할 요소들을 파악하여 각각의 위험성 검토
  - ▸ 개인정보 수집기관과 활용기관이 동일하여 우연한 재식별이 발생할 수 있는 위험성, 가명정보취급자가 우연히 아는 사람을 식별할 가능성 등

재식별 시 영향도 위험성 검토

- 데이터 특성*에 따른 재식별 위험성의 증가, 재식별이 발생하는 경우 사회적 파장 등 재식별 영향도를 추가적으로 검토

  * 민감한 분야 및 사회적 영향도가 높은 분야 직업군 등

[체크리스트 기반의 위험성 검토]

위험성 검토는 개인정보처리자의 상황에 따라 적절한 방법을 선택하여 수행할 수 있으며 검토 수준 객관성을 확보하기 위해 처리환경 및 데이터 자체 식별 위험성 검토를 체크리스트* 기반으로 수행 가능

- ▸ 위험성 검토와 관련하여 '위험성 검토 체크리스트 예시'(별지 10)을 참고하여 체크리스트 기반으로 처리환경 및 데이터 자체에 대한 위험성 검토를 실시할 수 있음
  - * 체크리스트는 위험성 검토가 어려운 기관을 위해서 제공하는 최소한의 검토 방식이며 체크리스트는 복합적 상황에 대한 위험성 검토가 어려운 부분이 있으므로 각 기관의 내부 상황 및 특성을 고려하여 체크리스트 내 항목을 가감하거나 혹은 추가적인 복합 위험성 검토 노력을 기울여야 함

※ 체크리스트를 활용한 위험성 검토는 교육부 개인정보보호 포털 참고자료에서 가명정보 처리 실무안내서 참조

[데이터 식별 위험성 검토]

○ 개인정보 항목 위험성 검토

- 기관 자체적으로 개인정보 분류체계를 작성하거나 교육부에서 제공하는 목록*을 바탕으로 해당 항목별 위험성을 분류하여 적용

* (별지 13) 교육기관 분류체계별 개인정보 항목별 위험성 목록 참조

분류체계	항목명	위험성	검토의견	처리강도
고유식별정보	운전면허번호	10	목적에 필요없음	매우강함
개인식별정보	학번	7	식별자로 필요 (표준 처리수준 및 처리방안 적용)	강함
개인식별가능정보	주소	6	식별자로 필요 (표준 처리수준 및 처리방안 적용)	중간
…	…			…

[표 5] 개인정보 항목 분류체계 위험성 예시

※ 상기 분류체계표는 항목 자체에 대한 것으로 여러 항목의 구성 및 분포에 따라 변경될 수 있음

- 처리대상 정보집합물 내 데이터의 구성 및 분포에 따른 재식별 위험을 추가적으로 검토
- 처리대상 정보집합물에서 특이정보 등을 검토하여 재식별 위험을 추가적으로 검토(특이정보가 많을수록 식별될 위험성 증가)

식별 위험성 검토 결과보고서 작성

○ **(가명정보 식별 위험성 검토 결과보고서 작성)** 가명정보처리자는 가명정보 처리 환경 위험성과 항목별 위험성을 종합적으로 고려하여 가명처리에 대한 위험성 검토 결과를 도출

- 위험성 검토 결과를 기반으로 '가명정보 식별 위험성 검토 결과보고서'(별지 1) 작성 및 관리

• 식별 위험성 검토 항목별 조치 방안

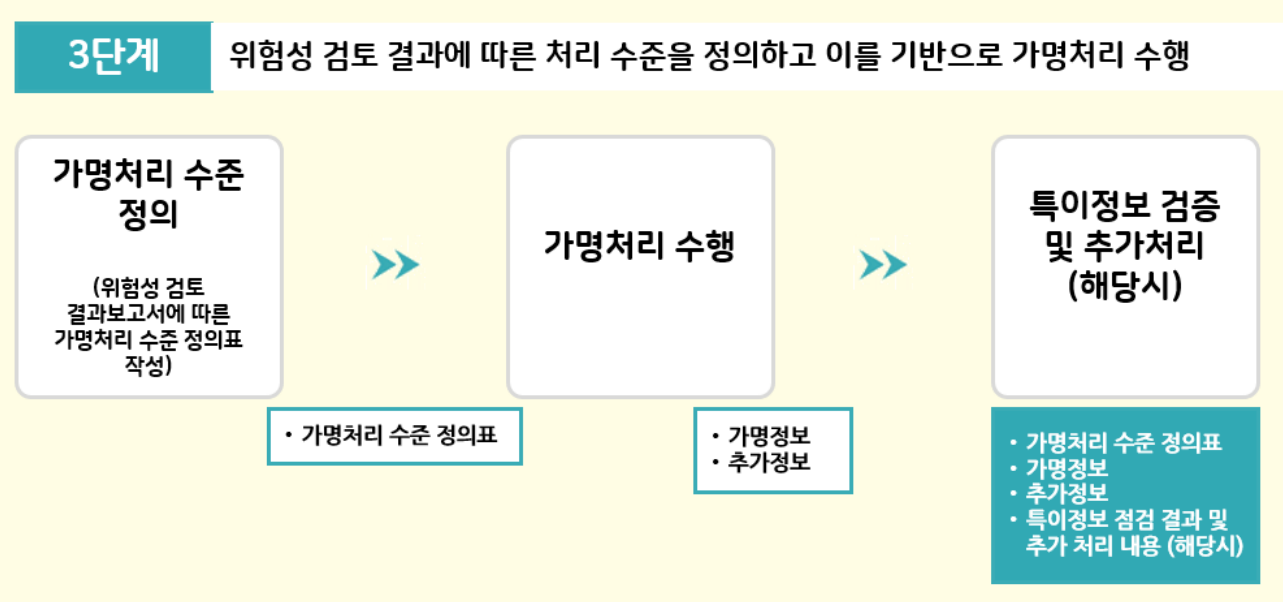
구분		조치 방안
항목	세부 항목	
필수 요건	가명처리 과정	위험성 발생시 해당 위험을 즉시 조치
	이용기관의 보호수준	법적 준수사항 조치
처리 환경	가명정보 처리 장소 및 형태	위험도가 낮은 장소에서 가명정보를 처리하도록 하고 불가능한 경우 가명처리 수준 높여 위험도를 경감
	다른 정보	가명정보를 처리하는 장소에서는 다른 정보에 대한 접근 및 소지를 금지
	이용기관의 신뢰도	이용기관의 신뢰도가 낮은 경우 높은 수준의 가명처리를 수행
	재식별 영향도	재식별 영향도 관련 위험성이 높은 경우 반드시 필요하지 않다면 삭제(해당 값, 레코드 또는 컬럼)하거나 일반화 수행
	우연한 재식별	우연한 재식별 방지를 위해 유사 경험이나 개인정보 취급자에 대해 제한하거나 보안서약서 등의 관리적 보호조치를 추가 적용
데이터	개인정보 항목	삭제를 원칙으로 하고 목적상 반드시 필요한 경우에만 가명처리 수준을 높여서 수행
	데이터 구성	데이터 항목수 감소, 데이터 구성(컬럼별 연계합 정보) 연결 수치 감소, 모집단의 규모 및 규모 대비 샘플 규모 등의 위험도를 낮추고 연결 시간 특성을 갖추지 않거나 낮추도록 조치
	데이터 분포	특이값이 발생하는 영역에 대해 원칙적으로 삭제처리하고 반드시 필요한 경우에는 상하단 코딩, 범주화 등으로 처리

[표 6] 식별 위험성 검토 항목별 조치 방안

주요 산출물

- 가명처리 대상 목록
- 가명처리 과정 검토 확인서
- 이용기관의 개인정보 보호수준 검토 확인서
- 처리환경 식별 위험성 검토서(또는 체크리스트)
- 데이터 식별 위험성 검토서(또는 체크리스트)
- 가명정보 식별 위험성 검토 결과보고서

2-3 가명처리(3단계)



<그림 4> 가명처리 단계 세부 절차

가명처리 수준

- **(가명처리 수준 정의)** '가명정보 식별 위험성 검토 결과보고서'(별지 1)를 기반으로 적절한 가명처리 방법과 수준을 결정하고 '가명처리 수준 정의표'(별지 2) 작성

가명처리 수준 정의 및 가명처리 수행

- **(가명처리 수행)** '가명처리 수준 정의표'(별지 2)를 기반으로 다양한 가명처리 기술을 적용하여 가명처리 수행

• 가명처리 단계에서 생성되는 추가정보는 삭제하는 것을 원칙으로 하되, 시계열 분석 등과 같이 불가피하게 저장하여야 하는 경우 분리·보관한다.

※ 세부사항은 II편 〉 3. 가명정보 안전조치 〉 기술적 보호조치 참고

※ '가명정보 식별 위험성 검토 결과보고서' 또는 '가명처리 수준 정의표'에는 프라이버시 보호모델 (k-익명성 등) 적용 여부 등을 추가할 수 있음

특이정보 검증 및 추가처리(해당시)

- **(특이정보 검증)** 가명처리된 정보에서 개인이 식별될 가능성이 높은 특이정보를 확인

- **(특이정보 처리)** 특이정보가 확인된 경우 특이정보에 대한 레코드 또는 컬럼 삭제, 범주화 등 가명처리 목적을 달성할 수 있는 범위 내에서 추가적으로 필요한 가명처리 수행

  - ▸ 수능 만점자, 국내 최고령, 최장신, 고액 체납금액, 고액 장학금 기부자 등 전체적인 패턴에서 벗어나 극단값이 발생할 수 있는 정보
  - ▸ 희귀 성씨, 희귀 혈액형, 희귀 눈동자 색깔, 희귀 병명, 희귀 직업 등 정보 자체로 특이한 값을 가지고 있는 정보 등

※ 특이정보 처리 사례는 개인정보보호위원회 『가명정보 처리 가이드라인』의 '참고자료 2. 특이정보 처리 사례'를 참조하여 처리

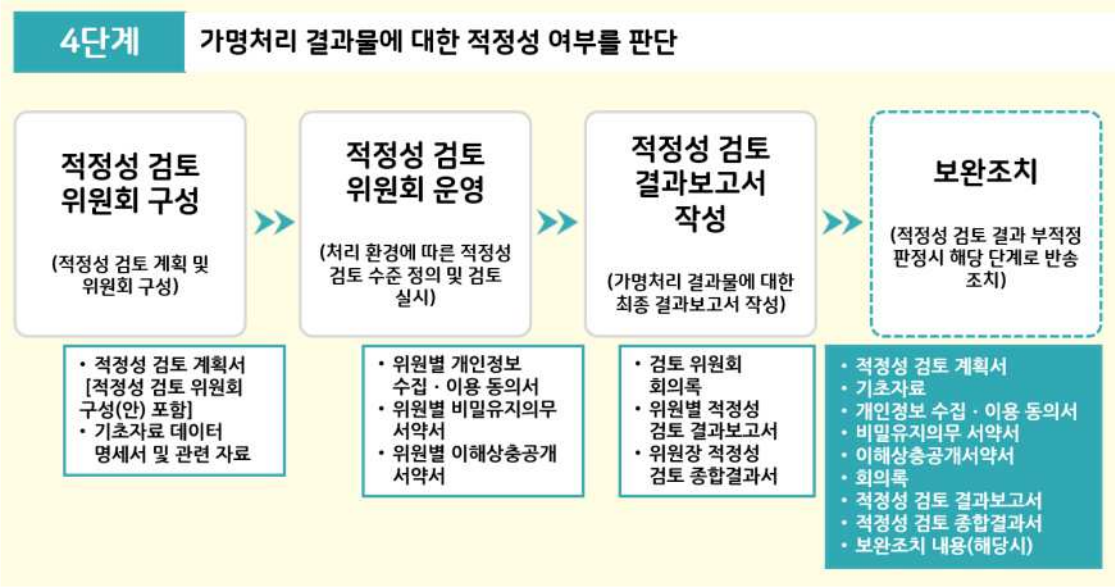
- 특이정보를 처리하는 과정에서 변경사항 발생 시 필요한 경우 기존에 작성된 '가명정보 식별 위험성 검토 결과보고서'(별지 1)나 '가명처리 수준 정의표'(별지 2)에 해당 내용 반영

- **(목적 달성을 위한 추가 가명처리)** '가명정보 이용제공 신청서'(별지 12)의 '첨부 2. 활용데이터 요구 수준표' 등을 참고하여 목적 달성이 어렵다고 처리자가 판단되는 경우 필요한 수준을 고려하여 추가 가명처리 수행

주요 산출물

- 가명처리 수준 정의표
- 가명정보, 추가정보
- 특이정보 점검 결과 및 추가처리 내용(해당시)

2-4 적정성 검토(4단계)



<그림 5> 가명처리 적정성 검토 단계 세부 절차

적정성 검토 위원회 구성

○ 가명정보처리자는 처리된 가명정보의 적정성 검토 등을 위해 적정성 검토 위원회(이하 “위원회”라고 한다.) 구성* 권장

* 내부활용의 경우 등 위험성이 낮다고 판단하여 내부관리계획 등에서 정한 경우 별도 위원회 구성없이 내부의사결정 절차에 따라 적정성 검토 및 승인 가능

- **(위원 자격 및 인원)** 개인정보보호, 가명처리 기법 등에 관한 학식과 경험이 풍부한 사람으로 다음 각 호에 해당하는 사람을 고루 포함하여 3명으로 구성하며 필요시 7명까지 위원을 확대하여 구성 가능

1. 개인정보 보호와 관련한 업무 경력이 있거나 관련 단체로부터 추천을 받은 사람
2. 개인정보처리자로 구성된 단체에서 활동한 경력이 있거나 관련 단체로부터 추천을 받은 사람
3. 그 밖에 개인정보 보호 또는 개인정보 활용과 관련한 경력 및 전문성이 있는 사람

※ 『가명정보의 결합 및 반출 등에 관한 고시』(개인정보보호위원회 고시) 〉 별표 1 결합전문기관 지정 기준 〉 2호의 자격 기준 준용 가능

- **(역할 및 기능)** 가명처리, 가명정보 처리의 적정성 및 가명정보를 제3자에게 제공하는 경우 제공의 적정성 등 검토

- **(위원장)** 위원 중 호선으로 정하거나 위원으로 임명된 가명처리기관의 개인정보 보호책임자 또는 그에 준하는 임직원

○ 내·외부 전문가로 위원 구성 시 비율은 기관별 업무 성격 등에 따라 탄력적으로 구성하되, 교육분야 각급기관* 이외에 가명정보 제공 시에는 반드시 외부 전문가를 포함하여 구성

* 『교육분야 가명·익명정보 처리 가이드라인』 적용범위(p.3) 참고

적정성 검토 위원회 운영

○ 위원회는 적정성 검토 필요 발생 시 구성·운영하도록 하며, 개인정보처리자는 사전에 이에 대한 인력풀을 구성·운영 가능

※ 단, 소규모 단위 또는 전문인력 부재 등으로 인하여 가명정보 처리 지원이 필요한 기관(학교 등)의 경우는 상급기관(교육지원청 등) 또는 교육분야 개인정보보호 전문기관을 통해 지원*을 받을 수 있음

* 적정성 검토 위원 인력풀 제공 또는 적정성 검토 지원(위원회 구성, 위원 참여 등) 등

○ 가명정보처리자는 적정성 검토를 위한 기초자료*를 준비

* 사업계획서, 가명정보 식별 위험성 검토 결과보고서, 가명처리 수준 정의표 등이며 세부 목록은 '개인정보 가명처리 적정성 검토 양식'(별지 12) 참조

기초자료에 포함할 내용	기초자료명 예시
사용 목적	사업계획서
이용 환경(개인정보보호 수준, 보유 정보 등)	
가명처리 대상 정보집합물 및 가명정보 명세	가명처리 정보집합물
개인정보 항목별 적용 가명처리 기법	가명정보 식별 위험성 검토 결과보고서, 가명처리 수준 정의표
가명처리 방법 및 수준	가명처리 수준 정의표
기타 프라이버시 보호모델 적용 여부 등이 기초자료에 포함이 가능	가명처리 수준 정의표 또는 가명정보 식별 위험성 검토 결과보고서

[표 7] 기초자료에 포함될 내용별 예시

○ 적정성 검토 위원들은 안전한 물리적 또는 논리적 공간에서 준비된 기초자료를 기반으로 적정성 검토 실시

적정성 검토 사항
① 가명처리 자체의 적정성뿐만 아니라 목적 달성을 위한 최소한의 가명정보 만으로 생성되었는지, 재식별 가능성 여부 검토
② 통계작성, 과학적 연구, 공익적 기록보존을 위하여 가명정보를 제3자에게 제공하는 경우 제공받는 자가 보유한 다른 정보와의 결합을 통한 식별가능성, 가명정보 보호수준, 신뢰도 등을 고려하여 가명정보의 제공이 적정한지 종합적으로 검토

※ 적정성 검토를 위한 자료는 개인정보에 해당하므로 개인정보 보호법에 따라 반드시 위원회 위원들을 대상으로 이해상충 공개 서약서, 보안서약서 등 징구

- 적정성 검토 위원회는 회의록 작성과 함께 아래의 세부 절차에 따라 적정성 검토 수행

<그림 6> 적정성 검토 위원회 운영 세부 절차

적정성 검토 결과보고서 작성

- 위원회는 적정성 검토 수행 결과에 대해 기초자료 등을 참고하여 '적정성 검토 결과보고서(위원용)'(별지 12)와 '적정성 검토 종합 결과서'(별지 12)를 작성

보완조치

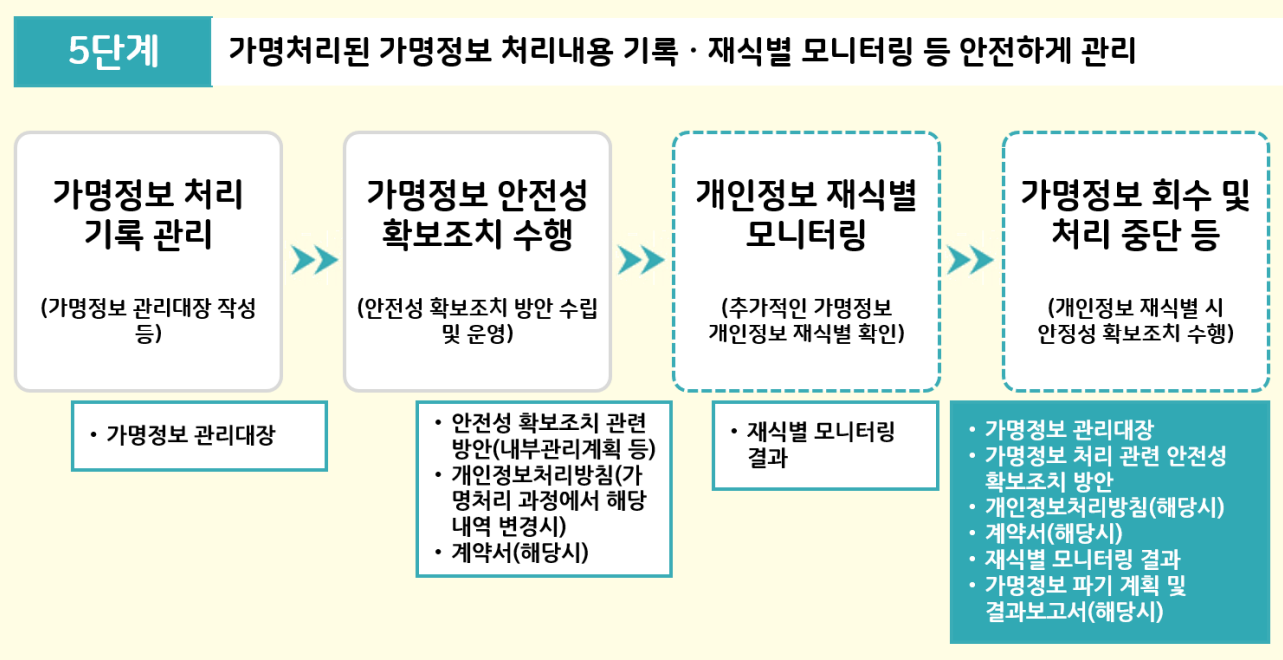
- 적정성 검토 결과 "부적정" 판정 시 가명정보의 활용·제공 계획을 중단하거나, 가명정보 활용을 계속하고자 한다면 "부적정"에 해당하는 단계로 돌아가서 보완조치를 단계적으로 수행한 후 다시 적정성 검토를 하여 "적정" 판정을 받아야 함

※ 적정성 검토 과정에 개인 식별 위험이 발생한 경우 위원회 판단에 따라 즉시 조치가 가능한 경우 즉시 조치 후 적정성 검토를 진행할 수 있음

주요 산출물

- 가명처리 적정성 검토 계획서(위원회 구성안 포함)
- 기초자료 데이터 명세서(목록) 및 관련 자료
- 개인정보 수집.이용 동의서
- 비밀유지의무 서약서, 이해상충 공개 서약서
- 적정성 검토 회의록
- 적정성 검토 결과보고서(위원용), 적정성 검토 종합결과서(위원장용)
- (해당시) 보완조치 내용

2-5 안전한 관리(5단계)



<그림 6> 안전한 관리 단계 세부 절차

- **(가명정보 처리 기록 관리)** 가명정보처리자는 가명정보 처리에 관한 내용*을 기록으로 작성하고 안전하게 보관·관리(별지 5 참조)

  * 가명정보의 처리 목적, 가명처리한 개인정보의 항목, 가명정보의 이용내역, 제3자 제공 시 제공받는 자, 처리 및 보유기간, 추가정보의 이용 및 파기 등

- **(가명정보 안전성 확보조치 수행)** 가명정보처리자(제공·활용하는 자)는 가명정보의 안전한 관리를 위한 내부관리계획의 수립 등 법령에서 요구하는 관련 조치 수행

  • 가명정보 처리 관련 사항을 내부관리계획에 포함하여 수립·시행해야 하며 사전 준비 단계에서 공개한 개인정보 처리방침 내용 변경이 발생한 경우 변경내역을 개인정보 처리방침에 적용

- **(개인정보 재식별 모니터링)** 가명정보처리자는 가명정보 보유기간 동안 개인정보 재식별 가능성이 증가하는지 여부 등을 지속적으로 모니터링하고 정기적으로 점검(연 1회 이상 권고)

- **(가명정보 회수 및 처리 중단 등)** 가명정보처리자(활용자)는 개인정보가 재식별된 경우 즉시 가명정보 처리 중단 및 즉시 삭제(파기) 등의 조치 수행

※ 필요시 개인정보처리자는 내부관리계획 또는 별도의 가명정보 처리 지침(기관 자체 수립) 등에 재발 방지 방안 수립 가능

<그림 7> 가명정보 회수 및 처리 중단 절차

※ 교육부 가명정보 처리 수준진단 및 관리

- 필요 시 가명정보 처리 현황조사 및 교육부 개인정보보호 수준진단을 활용하여 실태점검 등 실시

주요 산출물

- 가명정보 관리대장
- 가명정보 처리 관련 안전성 확보조치-내부관리계획 등 (기존에 존재할 경우 불필요)
- 개인정보처리방침 : 홈페이지에 해당 내용 공개 (사전준비 단계에서 공개한 내용이 변경된 경우)
- 계약서(제3자 제공 또는 가명정보 처리 위탁 등으로 타 기관에서 가명정보를 처리시)

  ※ 가명정보를 제3자에게 제공하는 경우 적정성 검토(4단계) 완료 이후 계약서를 작성하고 안전한 관리(5단계)에서는 작성한 '계약서'를 산출물로 관리(해당 시)
- 재식별 모니터링 점검 결과(연 1회 이상)
- 가명정보 파기 계획 및 결과보고서 : 재식별 모니터링 결과 재식별된 경우 안전조치 관련 내용 포함

3 가명정보 안전조치

관리적 보호조치

- **(가명정보 처리 내부관리계획 수립·시행)** 가명정보 처리 관련 내용*을 내부관리계획에 포함하고 시행

☞ **내부관리계획에 포함 사항**

가. 가명정보 또는 추가정보의 관리책임자 지정에 관한 사항

나. 추가정보 별도 분리 보관 (개인정보-가명정보-추가정보 모두 분리)

다. 가명정보 또는 추가정보의 안전성 확보조치에 관한 사항

라. 가명정보취급자의 교육에 관한 사항

마. 가명정보 처리 기록 작성 및 보관에 관한 사항

바. 개인정보 처리방침 공개에 관한 사항

사. 가명정보의 재식별 금지 등 오남용 제한 및 처벌에 관한 사항

아. 가명정보 재식별 발생 시 대응조치

※ 가명정보처리자는 내부 가명정보의 처리 중단·회수·파기뿐만 아니라 제3자에게 제공한 가명정보도 관련 절차에 따라 파기할 수 있는 내용 포함

* (별지 11) 내부관리계획 및 개인정보 처리방침 예시 참조

- **(개인정보처리방침 공개)** 관련 내용을 공개하고 변경 발생 시 즉시 재공개

☞ **개인정보처리방침에 포함 사항**

가. 가명정보의 처리 목적

나. 가명정보의 처리 및 보유 기간(필요시)

다. 가명정보의 제3자 제공에 관한 사항(해당 시)

라. 가명정보 처리의 위탁에 관한 사항(해당 시)

마. 처리하는 가명정보의 항목

바. 법 제28조의4에 따른 가명정보의 안전성 확보조치에 관한 사항

- **(취급자 관리 및 교육)** 가명정보취급자 관리·교육 실시

- 가명정보취급자 직무 분리 : 가명정보의 원본 개인정보 및 추가정보 접근 금지 등 취급자 분리
- 가명정보취급자에 대한 교육계획 수립 및 교육 실시 등

- **(가명처리 위탁 관리)** 가명정보 처리업무를 외부에 위탁하는 경우 수탁자 관리·감독을 위한 방안 마련 및 수행

  - 법 제26조에 따라 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항 등을 포함하여 수탁자 관리·감독 실시
  - 개인정보 처리업무 위탁계약서에서 요구하는 주요 항목 이외에 추가 사항* 반영

    * 가명정보 재식별 금지, 재식별 위험 발생 시 위탁사에 즉시 통지

- **(제3자 제공시 계약 주의사항)** 통계작성, 과학적 연구, 공익적 기록보존 목적으로 가명정보를 제3자에게 제공 시 보호대책을 마련하고 계약서에 주요 사항을 포함하여 시행

☞ **가명정보 제3자 제공 관련 계약서에 포함 사항**

가. 가명정보 처리 목적
나. 가명정보 처리 및 보유 기간
다. 가명정보 재식별 금지 및 재식별 발생시 통지
라. 가명정보 제3자 제공 금지(재제공 금지)
마. 가명정보 안전성 확보조치 준수
바. 가명정보 위탁 제한 (민간기업에 제공하는 경우에는 재위탁 금지)
사. 계약사항 위반시 손해배상 등 책임에 관한 사항
아. 가명정보 목적 및 기간 달성 시 즉시 파기에 관한 사항
자. 파기 후 파기내역 통보
차. 가명정보 제공자가 파기 요청시 즉시 파기 준수에 관한 사항(재식별 사고 및 계약 위반 사항에 한함)

※ 제공받는 기관이 교육행정기관 및 학교 등 민간이 아닌 경우 공문으로 대체 가능

- **(가명정보 관리대장 기록·관리)** 개인정보처리자는 가명정보를 처리(생성, 파기 등)하는 경우 '가명정보 관리대장'(별지 5)을 기록관리하고 연 1회 이상 점검

기술적 보호조치

- **(추가정보의 분리 보관)** 가명정보 처리 시 생성되는 추가정보는 삭제*하는 것을 원칙으로 하되, 불가피한 사유가 있는 경우 원본 개인정보, 가명정보와는 물리적으로 분리하여 보관

  * 추가정보 삭제 시, '가명정보 관리대장'(별지 5)을 활용하여 삭제내역 기록

※ 추가정보를 물리적으로 분리하기 어려운 경우 DB 테이블 분리 등 논리적으로 분리하는 것도 가능하나 엄격한 접근권한 관리 및 접근통제 적용

- **(접근 권한 관리)** 개인정보처리자는 가명정보 또는 추가정보에 접근할 수 있는 담당자를 가명정보 처리 업무 목적 달성에 필요한 최소한의 인원으로 지정하고 접근권한은 업무에 따라 차등 부여

※ 시행령 제29조의5(가명정보에 대한 안전성 확보 조치)제1항제3호 "가명정보와 추가정보에 대한 접근 권한의 분리"

- **(접속기록의 보관 및 점검)** 개인정보처리자는 가명정보 또는 추가정보 처리에 관한 접속 기록을 최소 1년 이상 보관·관리

※ 가명정보가 5만명 이상일 경우 최소 2년 이상 보관 등 법령 준수 필요

항목	접속기록 내용
계정	• 가명정보처리시스템에서 접속자를 식별할 수 있도록 부여된 ID 등 계정 정보
접속일시	• 접속한 시간 또는 업무를 수행한 시간
접속지 정보	• 가명정보처리시스템에 접속한 자의 컴퓨터 또는 서버의 IP 주소 등
처리한 정보주체 정보	• 가명정보취급자가 어떠한 가명정보를 처리하였는지를 알 수 있는 식별정보(가명정보 ID, 일련번호 등) • 가명정보는 일반적으로 대량의 정보를 처리하는 경우가 많으므로 대량의 정보를 처리 시 해당 검색조건문(쿼리)을 정보주체 정보로 기록 가능 • 가명정보의 특성상 추가정보의 사용 없이는 정보주체 식별이 불가능하므로 본 항목에는 실제 정보주체의 정보가 아니라 어떠한 가명정보를 처리했는지 추적할 수 있는 정보를 기록 가능
수행업무	• 가명정보취급자가 가명정보처리시스템을 이용하여 가명정보를 처리한 내용을 알 수 있는 정보(조회, 입력, 수정, 삭제, 다운로드, 출력 등)를 기록 • 가명정보의 재식별 행위를 파악할 수 있는 내용 기록

[표 8] 접속기록 포함 내용 예시

- 접속기록에는 가명정보취급자가 가명정보처리시스템에 접속하여 처리한 업무내역을 알 수 있도록 주요 정보 등을 모두 포함하고 월 1회 이상 주기적으로 확인

물리적 보호조치

(가명정보 및 추가정보에 대한 출입통제) 개인정보처리자는 가명정보 또는 추가정보의 안전한 관리를 위하여 물리적 안전조치 수행

- 전산실이나 자료보관실 등에 보관하는 경우 비인가자의 접근으로부터 보호하기 위해 출입통제 등의 절차를 수립·시행
- 가명정보 또는 추가정보가 물리적 공간을 이동*하는 경우 이를 고려하여 내부관리 계획에서 관리 절차를 수립·시행

  * 가명정보 공간으로의 다른 정보 반입, 기타 공간으로 가명정보의 반출, 가명정보 처리 공간 간의 가명정보 이동 등

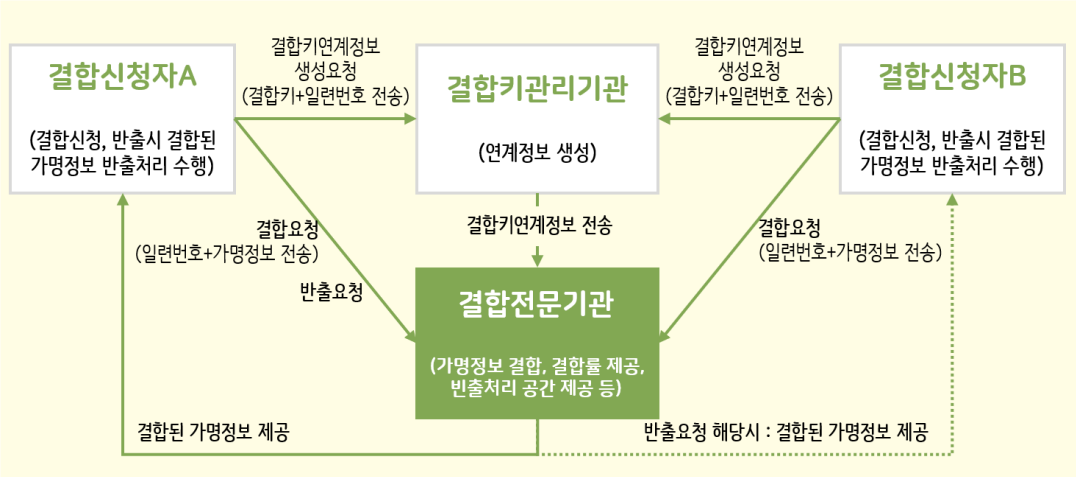
- 가명정보 또는 추가정보를 보조저장매체에 저장하는 경우에는 암호화를 적용하고 잠금장치가 있는 안전한 장소에 보관하여야 하며 보조저장매체 등에 대한 반·출입 통제 등 보안대책 마련

4 가명정보 결합

서로 다른 개인정보(집합물) 2개 이상을 가명처리하여 하나로 결합하여 이용할 수 있으며 이 경우 서로 다른 개인정보처리자 간 가명정보 결합을 외부결합이라 하고, 기관 내부에서 이용하는 가명정보 간 결합을 내부결합이라 한다.

외부결합 : 서로 다른 개인정보처리자 간 가명정보 결합·반출 절차

- 서로 다른 개인정보처리자 간의 가명정보 결합은 개인정보보호위원회 또는 중앙행정기관의 장이 지정하는 결합전문기관을 통해 수행



<그림 8> 결합전문기관을 통한 가명정보 결합 개념도

[가명정보 결합 기관 및 대상 예시]

서울시교육청이 등하교 시간과 학업성취도와의 상관관계를 연구하여 그 결과를 바탕으로 학생 배치, 노선 변경 요구 등을 진행하려는 경우

☞ 서울시교육청은 서울시교통공단이 보유한 교통카드 기록과 가명정보 결합

- 결합신청기관 : 서울시교육청(활용(주관)기관), 서울시교통공단(제공기관)
- 결합대상 : 교육청(학생성적), 교통공단(교통카드 기록)

- 서로 다른 개인정보처리자간의 가명정보 결합 세부 절차 및 진행은 개인정보보호위원회 가명정보 처리 가이드라인을 참고하거나 해당 결합전문기관에 문의하여 진행

※ 교육분야 결합전문기관 : 한국교육학술정보원(privacydid@keris.or.kr, '22년 7월 기준)

내부 결합 : 기관 내부의 가명정보 결합

○ 개인정보처리자는 자신이 보유하고 있는 가명정보를 결합하여 활용할 수 있으며, 결합절차가 별도로 정해져 있지는 않지만 결합 과정에서 특정 개인을 알아볼 수 없도록 유의하여 결합 수행

- 안전한 결합을 위해 결합키를 이용한 결합 방법 선택 가능
- 결합 과정에서 가명정보가 재식별되지 않도록 권한 분리를 활용하도록 권장

○ 일반적으로 가명정보의 내부 결합 절차는 다음과 같음

<그림 9> 가명정보 내부결합 절차

- 개인정보처리자는 결합된 정보를 활용할 때 특별한 사유(시계열 분석 등)가 없는 한 결합키 등 결합을 위해 사용한 정보를 삭제한 후 활용

※ (주의) 결합키 생성에 이용된 알고리즘, 매핑테이블 등은 추가정보에 해당하므로, 삭제하거나 결합된 가명정보와 분리하여 보관하여야 하고, 접근권한 분리 필요

<그림 10> 결합키를 이용한 가명정보 내부결합 예시

Chapter

III

익명처리

Ⅲ 익명처리

1 개요

익명정보는 더 이상 개인정보로 취급하지 않기 때문에 개인정보 보호법 등 관련 법령의 제한을 받지 않고 자유롭게 활용 가능

※ 단, 익명정보 활용을 위해서는 보다 명확하고 엄격한 처리와 객관적인 검증이 요구됨

익명처리 원칙

- 개인식별정보는 삭제하고, 개인식별가능정보는 원칙적으로 삭제하되 데이터 이용 목적상 꼭 필요한 경우에는 안전한 방식으로 익명처리 필요
- 익명처리 업무를 수행하는 자는 익명처리 대상 개인정보를 처리하는 업무 수행 금지. 다만, 불가피한 사유가 있을 경우 보완통제 대책을 수립하여 관리자의 승인하에 제한적으로 취급 가능
- 개인정보처리자는 익명정보 적정성 검토를 수행하는 경우 가명정보 적정성 검토 위원회와 동일한 절차로 구성하여 운영 가능
- 익명정보처리자는 '익명정보 관리대장'(별지 6)을 기록·관리하고 개인정보처리자는 연 1회 이상 점검(해당 시)

☞ **익명정보 관리대장 포함 사항**

가. 익명처리한 날짜

나. 익명정보의 항목

다. 익명처리한 사유와 근거

라. 익명정보를 제3자 제공한 경우 제공받은 자와 제한사항 (공개한 경우 공개처 등)

○ 개인정보가 포함된 공공데이터는 특정 개인을 식별할 수 있는 요소를 삭제하거나 익명처리(적정성 검토 포함) 후 개방

- 원칙적으로 그 자체로 개인을 식별할 수 있는 정보는 삭제
- 개방대상 정보에 이미 공개된 정보 등과 결합하여 개인 식별이 가능한 정보가 포함되어 있는지 여부 등을 사전에 검토
- 이미 개방한 데이터가 다른 정보와 결합하여 개인 식별이 가능한 지 여부 등을 주기적으로 모니터링 한 후 재식별이 되는 경우 해당 개인정보 삭제 또는 익명처리

※ 『공공데이터의 제공 및 이용 활성화에 관한 법률』, 『공공데이터 관리지침』에 명시된 개인정보 등 비공개 대상정보의 포함 여부 확인 절차 등을 준수해야 함

익명정보 재식별 위험과 적정성 충족 여부에 대한 책임성

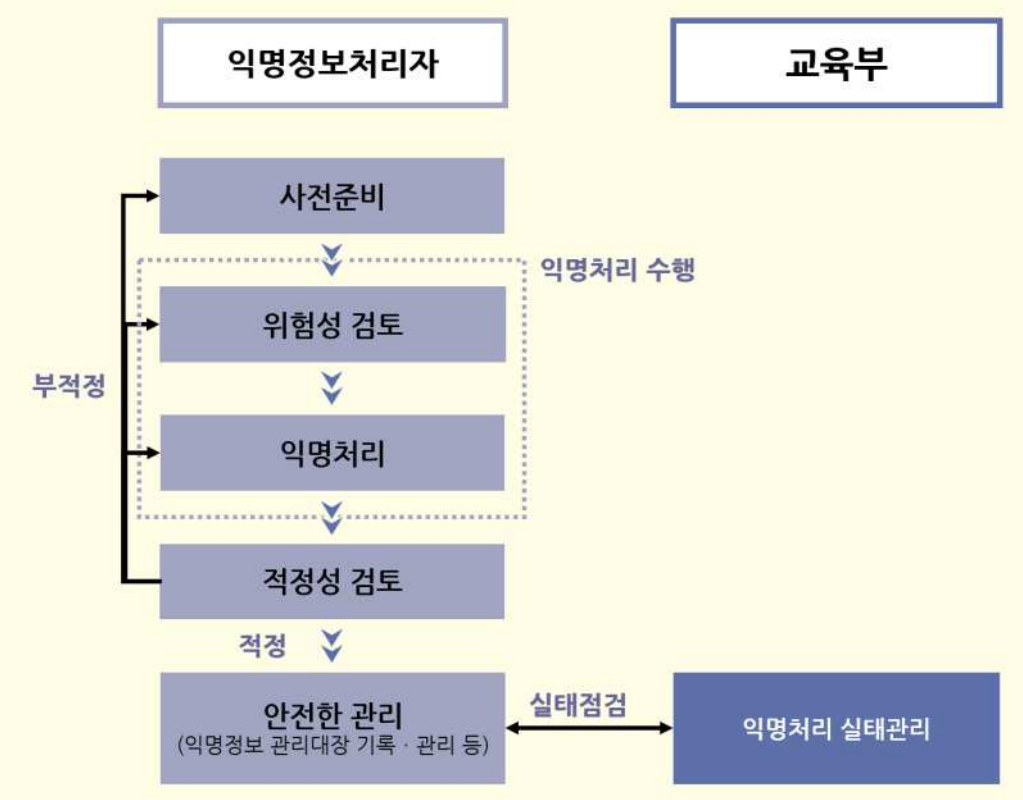
- 개인정보는 익명처리하여 익명정보를 만들었다고 하여도 시간이 지남에 따라 다른 정보와 결합하여 개인정보가 재식별될 수 있음
- 시간이 지남에 따라 결합용이성과 입수가능성이 증가하여 유형별 재식별 위험이 증가(ISO/IEC 20889에 따른 분류 위험)

유형 구분	재식별 위험				
	식별가능성	복원가능성	특정가능성 (Single Out)	추론가능성 (Linkability)	연결가능성 (Inference)
가명정보	없음	없음	존재	존재	존재
익명정보	- (NA)	- (NA)	없음	없음	없음

[표 9] 가명정보 및 익명정보의 재식별 위험 요소 분류 예시

- 익명정보 적정성 검토를 거쳤다고 하여도 개인정보 보호법 제58조의2에 해당하는 "개인을 알아볼 수 없는 정보"가 되었다는 입증 책임은 개인정보처리자에 있음
- 따라서, 개인정보처리자는 익명정보를 생성하고자 하는 경우 안전한 처리를 할 수 있도록 주의를 다해야 함

익명처리 절차 개념도



<그림 11> 익명처리 절차

- **(사전준비)** 익명처리 목적을 명확히 정의하고 익명처리 대상 개인정보 선정
- **(익명처리 수행)** 익명처리 수준을 정의하고 수준에 맞도록 익명처리 기법을 활용하여 개인정보를 익명처리
- **(적정성 검토)** 익명처리 수준 등에 맞는 익명처리가 되었는지 여부 및 익명정보 내 개인정보 식별 여부 및 재식별 가능성 검토
- **(안전한 관리)** 익명처리된 익명정보에 대해 기록·관리하고 재식별 발생 시 대응할 수 있도록 대책 수립 가능
- **(익명처리 실태관리)** 익명처리 기록·관리 등에 관한 사항을 조사 및 점검 실시

익명처리 예시

[원본정보 예시]

성명	연락처	성별	생년월일	혈액형		전공	학위
				ABO	RH		
김영희	090-1234-5678	여	19650512	A	Rh+	법학	박사
강순희	090-8525-4564	남	19671212	B	Rh+	컴퓨터	학사
최복례	090-8546-5456	여	19681015	O	Rh+	건축	학사
홍길동	090-5524-1325	남	19920721	AB	Rh-	보안	학사
이홍준	090-6974-1235	남	19930423	AB	Rh+	교육	학사
김신우	090-3456-7890	남	19940925	O	Rh+	음악	학사
...	...	...	...	...	...	...	...

[표 10] 원본정보 예시

[익명처리 예시]

성별	혈액형		전공	학위	익명성
여	A	Rh+	법학	학사	동질집합 k = 30 이상
여	A	Rh+	법학	학사	
...	...	...	...	...	
여	B	Rh+	법학	학사	
여	AB	Rh+	교육	학사	
여	O	Rh+	음악	학사	
여	A	Rh-	법학	학사	
...	...	...	...	...	

[표 11] 익명처리 예시 과정(1)

⇩

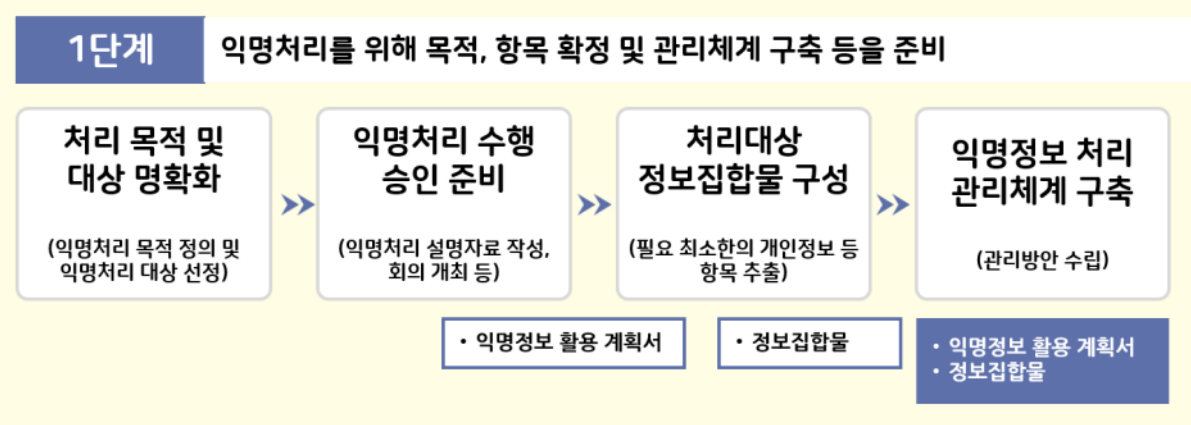
성별	혈액형		전공	학위	통계 (단위, 명)
여	A		법학	학사	550
여	A		법학	석사	310
...	...		...	...	...
여	B		법학	학사	251
여	AB		교육	석사	180
여	O		음악	박사	115
여	A	Rh-	법학	학사	151
...	...		...	...	...

[표 12] 익명처리 예시 과정(2)

- 성별·혈액형별 전공과 학위 현황의 익명정보를 만들겠다는 목적으로 프라이버시 보호모델 k-익명성* 값은 30 이상으로 설정
  * k-익명성이란 특정인임을 추론할 수 있는지 여부를 검토하여 일정 확률 수준 이상 비식별 되도록 하는 것을 의미하며 동일한 값을 가진 레코드가 최소한 k개 이상 존재하도록 하여 프라이버시를 보호하는 모델을 말함
- '성명', '연락처'는 특정 개인이 식별 가능하므로 삭제 처리
- '성별'은 활용 목적에 필요한 항목으로 유지
- '생년월일'은 활용 목적에 필요한 항목이 아니므로 삭제
- '혈액형'은 활용 목적에 필요한 항목이므로 유지. 다만, Rh-의 경우 희귀 혈액형 유형으로 개인이 식별될 가능성이 있는 경우 해당 레코드 삭제
  ※ Rh-를 모두 레코드 삭제를 하게되는 상황이 발생하면 Rh+만 남게되고 이 경우 사실 Rh의 분류는 의미가 없어짐. 따라서 활용 목적에 따라 이런 경우 Rh 항목에 대해 전체 삭제하는 것으로 일부 레코드 삭제를 방지할 수 있음
- '전공', '학위'는 결과 도출을 위한 항목이므로 유지. 다만, 개인이 식별될 가능성이 있는 경우 k-익명성에서의 k값은 30 이상이 나오도록 범주화하여 통계처리

2 익명처리 세부 절차

2-1 사전준비(1단계)



<그림 12> 사전준비 단계 세부 절차

- **(처리 목적 및 대상 명확화)** 익명처리를 하고자 하는 목적을 명확히 정의하고 익명처리 대상 정보 선정

※ 일반적으로 익명처리를 하게 되면 거의 통계성 정보만 남음

- **(익명처리 수행 승인)** 익명처리를 위하여 관련 자료(사업계획서 등)를 작성하고 내부 회의 개최 등을 통해 최종적으로 기관장 또는 개인정보 보호책임자 승인 후 진행

☞ **주요 처리 사항**

- 기관 외부에 익명정보를 제공하는 경우 개인정보 재식별 시 즉시 익명정보 사용 중단, 회수 및 파기에 관한 사항과 익명정보 제공자가 요청 시 즉시 파기하도록 하는 내용을 계약서(안)에 포함하여 사업계획서 작성

- **(처리 대상 정보집합물 구성)** 익명처리 목적 달성을 위해 필요한 최소한의 항목을 추출하여 익명처리 대상 정보집합물 구성

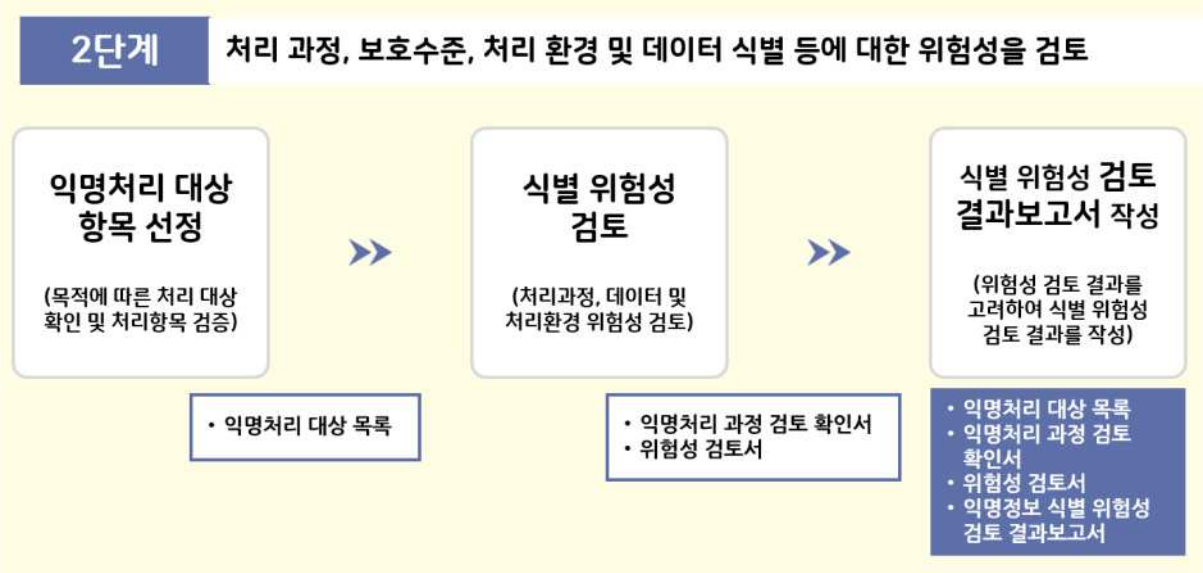
- **(익명정보 처리 관리체계 구축)** 익명정보를 생성하는 과정 및 익명정보 활용 과정에서 발생할 수 있는 위험을 안전하게 보호할 수 있는 관리방안* 수립

* 재식별 발생 시 처리 방안, 익명정보 관리대장 기록 및 관리자 지정 등에 관한 사항 포함 가능

주요 산출물

- 사업계획서 (제3자 제공인 경우 '익명처리 안전한 관리'에서 익명정보 제3자 제공 시 제한사항 참조)
- 처리대상 정보집합물(개인정보)

2-2 위험성 검토(2단계)



<그림 13> 위험성 검토 단계 세부 절차

익명처리 대상 항목 선정

- 사전준비 단계의 산출물에서 처리대상 및 대상별 특성을 확인하고 익명처리에 필요한 최소한의 항목을 추출

※ 개인식별정보에 해당하는 항목은 추출 금지

식별 위험성 검토

- **(처리과정 검토)** 익명정보 처리 과정을 확인하여 위험성 요소 검증 및 제거
- **(항목 분류 및 위험성 검토)** 개인정보 항목별 위험성 분류표 구성과 항목별 위험성을 검토

- 가명처리 검증 기준인 식별가능성이 있거나 복원가능성이 있는 항목은 원칙적으로 삭제하여 분류 대상에서 제외
- 삭제하지 않은 항목들을 중심으로 익명처리 검증 기준에 해당하는 특정가능성, 추론가능성, 연결가능성을 통한 재식별 위험을 고려하여 위험성을 검토

[항목별 위험성 분류 예시]

· ○○교육청이 A부서의 개인정보를 익명처리하여 홈페이지상에 정책 통계자료로 공개할 경우

- 특정가능성, 추론가능성, 연결가능성을 검토하여 상·중·하 또는 다양한 스케일(1~10 등)로 구분하여 위험성을 분류할 수 있음

재식별 위험				
식별가능성	복원가능성	특정가능성	추론가능성	연결가능성
-	-	상	상	상
-	-	중	중	중
-	-	하	하	하

- 항목별로 재식별 위험을 매칭하여 위험성을 분류(항목 특성에 따라 특정 위험 가능성이 적용되지 않을 수 있음)

항목	재식별 위험		
	특정가능성	추론가능성	연결가능성
항목A	상	상	상
항목B	중	중	중
항목C	하	하	하

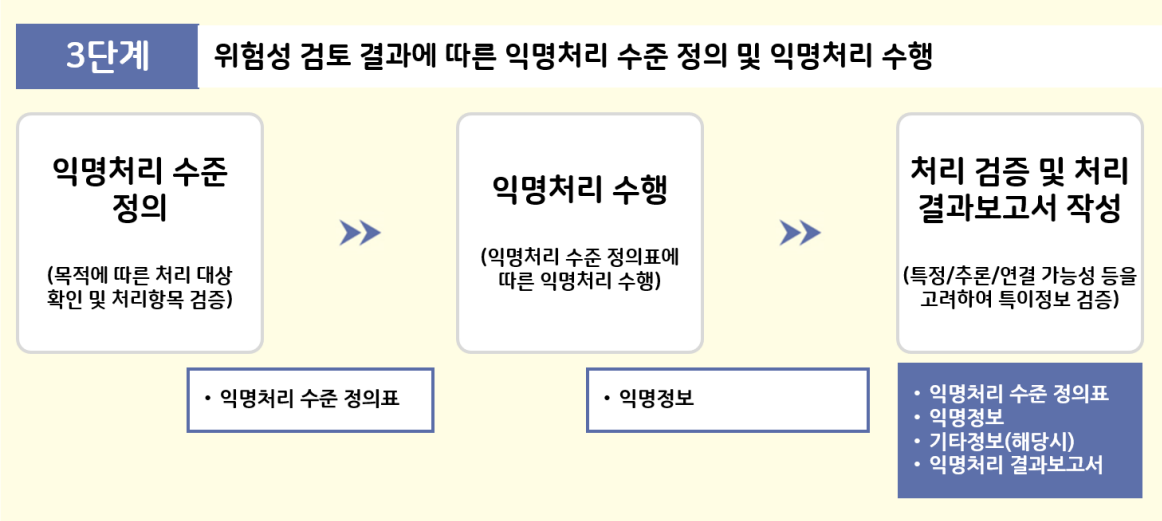
익명정보 식별 위험성 검토 결과보고서 작성

- 항목별 위험성 분류와 위험성 검토 결과를 고려하여 '익명정보 식별 위험성 검토 결과보고서'(별지 3) 작성

주요 산출물

- 익명처리 대상 목록
- 익명처리 과정 검토 확인서 및 위험성 검토서
- 익명정보 식별 위험성 검토 결과보고서

2-3 익명처리(3단계)



<그림 14> 익명처리 단계 세부 절차

익명처리 수준 정의

(익명처리 수준 정의) 개인정보 항목별 익명처리 수준 정의

- 기관 자체적으로 재식별 위험별 익명처리 수준 정의표를 작성하고 익명처리 대상을 항목별로 분류하여 적용 가능

[재식별 위험별 익명처리 수준 정의 예시]

· 기관 자체적으로 재식별 위험별 익명처리 수준 정의표 구비 가능

재식별 위험		익명처리 수준 예시
특정가능성	상	프라이버시 보호모델 익명성 k = 100 이상
특정가능성	중	프라이버시 보호모델 익명성 k = 50 이상
특정가능성	하	프라이버시 보호모델 익명성 k = 30 이상
추론가능성	상	…

· 항목 또는 속성별로 추론 가능성 위험을 매칭하여 익명처리 수준 정의

· 연결 가능성은 모든 항목의 동질집합에 대한 것을 종합적 고려 필요

(익명처리 수준 정의표 작성) 익명정보처리자는 '익명정보 식별 위험성 검토 결과보고서'(별지 3) 등을 종합적으로 고려하여 '익명처리 수준 정의표'(별지 4) 작성

- 항목별 재식별 위험뿐만 아니라 전체 항목의 재식별 위험성을 고려하여 '익명처리 수준 정의표'에 반영

※ 가장 높은 재식별 위험에 맞추어 수준 정의가 필요한 경우 등

익명처리 수행

- **(익명처리 수행)** 항목별 익명처리 수준을 확인하여 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없도록 익명처리 수행

- **(위험 제거)** 재식별 위험을 모두 고려하여 모든 가능성을 배제하도록 하여 개인이 재식별되는 위험을 제거

처리 검증 및 보고서 작성

- **(익명처리 검증 및 추가 익명처리 수행)** 익명처리 결과물에 대한 개인정보 재식별 가능성을 검증하고 재식별 가능성이 발생한 경우 추가 익명처리 수행

- 익명처리된 정보에서 개인이 식별될 가능성이 높은 특이정보를 확인하여 추가적으로 익명처리

※ 특이정보 처리 사례는 개인정보보호위원회 『가명정보 처리 가이드라인』의 '참고자료 2. 특이정보 처리 사례'를 참조하여 처리

- 특이정보를 처리하는 과정에서 변경사항 발생 시 필요한 경우 기존에 작성된 '익명정보 식별 위험성 검토 결과보고서'(별지 3) 또는 '익명처리 수준 정의표'(별지 4)에 해당 내용 반영

- 적정성 검토 결과 "부적정" 판정을 받은 경우 추가 익명처리 수행

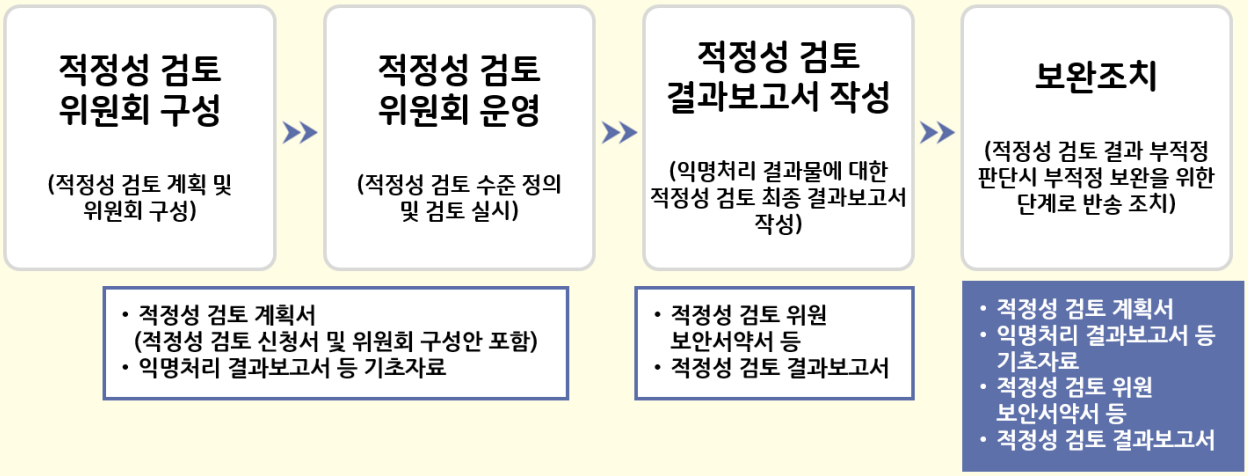
- **(익명처리 결과보고서 작성)** 개인정보 재식별 검증 결과 재식별 가능성이 없는 경우 적정성 검토를 위한 '익명처리 결과보고서'(기관별 자유양식)를 작성

주요 산출물

- 익명처리 수준 정의표
- 익명처리 결과보고서

2-4 적정성 검토(4단계)

4단계 익명처리 결과물에 대한 적정성 여부를 판단



<그림 13> 익명처리 적정성 검토 단계 세부 절차

○ 익명정보처리자는 익명정보 적정성 검토 등을 위한 위원회를 구성·운영하여 적정성 검토를 수행

- 익명처리에 대한 적정성 및 재식별 위험 등에 대한 검토

※ 세부 절차 및 방법은 '제Ⅱ편 가명처리 〉 2. 가명처리 세부 절차 〉 2-3. 적정성 검토'를 참고하고 그에 준하여 수행하되 프라이버시 보호모델을 추가하여 적정성 검토 수행 가능

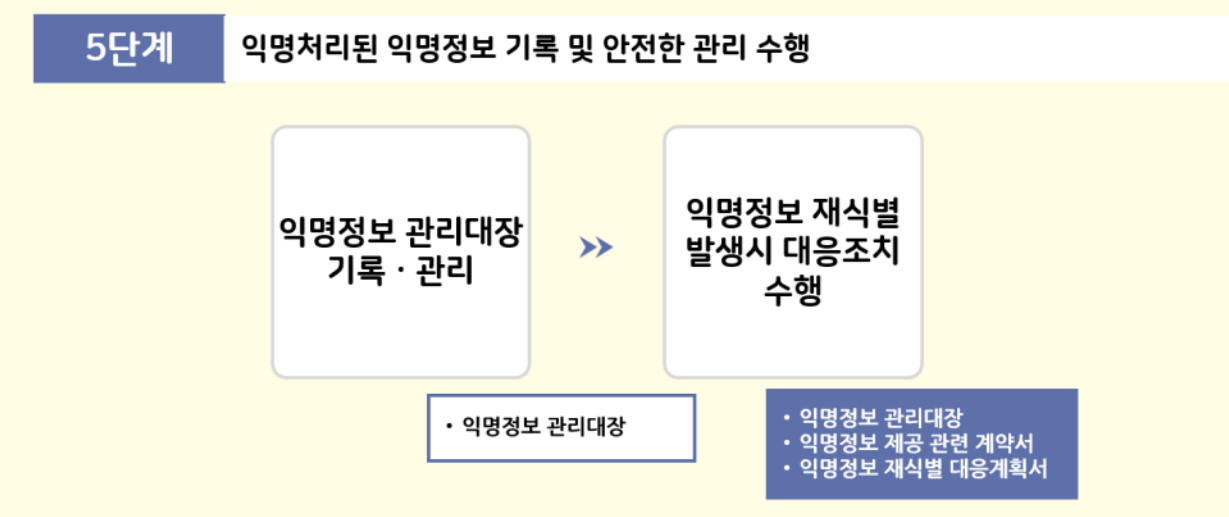
※ 단, 익명정보를 교육분야 각급기관 이외에 제공하는 경우에는 적정성 검토를 위한 위원회 구성 시 외부 위원을 과반수 이상 포함 구성

주요 산출물

- 익명처리 적정성 검토 계획서(구성안 포함)
- 익명처리 결과보고서 등 기초자료
- 비밀유지의무 서약서, 이해상충 공개 서약서, 보안서약서
- 적정성 검토 회의록
- 적정성 검토서 및 적정성 검토 결과보고서 (기관 자유양식)*

* 기존 가명처리 적정성 검토 결과서 양식을 준용하여 사용 가능

2-5 안전한 관리(5단계)



<그림 14> 안전한 관리 단계 세부 절차

- **(기록 관리)** 익명정보처리자는 익명처리에 관한 내용*을 기록(별지 6)하고 안전하게 보관·관리

  * 익명처리 기간, 항목, 사유 및 근거, 제공받는 자(해당 시), 제한사항, 익명처리 수행자, 책임자 등

  - 익명정보를 제3자에게 제공한 경우 재식별 발생 상황을 대비하여 추적 관리할 수 있도록 해당 사항을 '익명정보 관리대장'(별지 6)에 기록 및 관리

- **(재식별 발생시 대응조치)** 익명정보처리자는 익명정보 재식별 사고 발생 시 후속조치 수행

  - 익명정보 재식별 사고 발생 관련 대응 및 조치계획* 수립

    가. 재식별 사고 발생 시 즉시 익명정보의 사용 중단, 회수 및 파기

    나. 익명정보를 제3자에게 제공한 경우 제3자에게 해당 익명정보 즉시 사용 중단, 회수, 파기 및 파기 결과 회신 요청과 파기 결과 회신

  * 대응 및 조치 계획은 별도의 매뉴얼로 작성하는 것을 권고하며 어려울 경우 내부관리계획 등에 포함

  - 익명정보처리자는 익명정보를 제3자에게 제공 시 계약서 기반의 보호대책*을 수립하고 시행

  * 재식별 발생 상황을 대비하여 추적관리 및 회수 또는 파기할 수 있는 내용을 계약서에 제한사항으로 명시

- 익명정보 최초 제공자가 파기를 요청하는 경우 해당 익명정보를 사용하는 자는 누구든지 즉시 익명정보를 파기해야하고 그 결과를 최초 제공자에게 통보

(익명처리 관련 추가정보 파기) 익명정보 생성 시 재식별되지 않도록 익명처리 과정에서 재식별에 영향을 주는 정보는 본 가이드라인에서 별도로 기간을 명시하지 않은 경우 즉시 파기

주요 산출물

- 익명정보 관리대장
- 익명정보 제공 관련 계약서 (해당시)
- 익명정보 처리 관련 안전한 관리 계획서

※ 익명정보 재식별 시 대응 조치를 위한 계획으로, 사전준비 단계에서 작성한 사업계획서에 해당 내용이 포함되었을 경우 작성 제외

Chapter

Ⅳ

기타

Ⅳ 기타

부록1 주요 산출물 및 처리방안

가명처리

단계		내용	산출물	처리방안
1단계	목적 및 대상	가명처리 목적 및 가명처리 대상 개인정보 선정	가명정보 활용계획서 (제3자 제공시 계약서(안) 포함, 위수탁시 위수탁 계약서(안) 포함), 개인정보처리방침	기록물 관리에 따른 보유기간 내 보관
	승인 준비	사업 설명자료 작성, 내부 회의 및 사업 추진 타당성 검토(적합성 검토), 사업 승인 추진		
	정보집합물 구성	개인정보 항목을 선정하고 추출하여 정보집합물 구성	정보집합물	가명처리 후 삭제
	관리체계 구축	가명정보 보호대책 수립	내부관리계획,	준영구 보관
2단계	가명처리 대상 재선정(검증)	정보집합물에서 처리대상 및 대상별 특성을 확인하여 최소한의 항목을 추출	가명처리 대상 목록 (또는 정보집합물)	가명처리 후 삭제
	위험성 검토	필수요건 검토, 데이터 식별 위험성 검토, 처리환경 식별 위험성 검토 [위험성 검토 관련 서류] : 가명처리 과정 검토 확인서, 개인정보 보호수준 검토 확인서, 처리환경 식별 위험성 검토서, 데이터 식별 위험성 검토서	위험성 검토 관련 서류 등 (해당 시에는 위험성 검토 체크리스트 포함)	가명정보 이용기간 종료 후 3년간 보관
	가명처리 식별 위험성 검토 결과 보고서 작성	위험성 검토 결과에 따라 가명처리 검토 결과 보고서 작성	가명정보 식별 위험성 검토 결과 보고서 (별지 1)	

단계		내용	산출물	처리방안
3 단계	가명처리 수준 정의 및 가명처리 수행	가명처리 검토 결과 보고서 기반으로 가명처리 수준 정의표 작성, 가명처리 수준 정의표에 따른 항목별 가명처리 수행	가명처리 수준정의표 (별지 2), 특이정보점검 결과 및 추가처리 내용(해당 시)	가명정보 이용기간 종료 후 3년간 보관
			가명정보	이용기간 종료 후 삭제
			추가정보	즉시 삭제 권고 (보관 시 가명정보와 분리, 삭제 시 가명정보와 같이 삭제)
	보완조치	특이정보 등 재식별 가능성 확인 시 추가적으로 가명처리 (보완조치 수행 시 가명처리 수준 정의표 수정 반영)	가명처리 수준정의표	가명정보 이용기간 종료 후 3년간 보관
4 단계	적정성 검토 위원회 구성	적정성 검토 위원회 구성(3~7명)안을 포함한 적정성 검토 계획 수립	적정성 검토 계획서(위원회 구성안 포함)	기록물 관리에 따른 보유기간 내 보관
	적정성 검토 위원회 운영	적정성 검토를 위한 기초자료 준비 및 적정성 검토	(기초자료)	기초자료가 포함된 각 산출물 처리방안 참고
	적정성 검토 결과보고서 작성	적정성 검토 결과에 대한 결과보고서 작성	적정성 검토 결과보고서, 적정성 검토 종합결과서	가명정보 이용기간 종료 후 3년간 보관
	보완조치	적정성 검토 결과 부적정 판정 시 해당 단계로 반송 조치		
5 단계	가명정보 처리 기록·관리	가명정보 관리대장 기록·관리	가명정보 관리대장 (별지 5)	준영구 보관
	가명정보 안전성 확보조치 수행	가명정보 등에 대한 안전성 확보 방안 수립 및 운영 (개인정보처리방침 공개, 내부관리계획 수립 등)	안전성 확보조치 방안 (개인정보처리방침, 내부관리계획 등)	준영구 보관
			계약서 (해당 시)	법령에 따른 보유기간
	재식별 모니터링	가명정보를 처리 시 연 1회 이상 개인정보 재식별 여부 점검 수행	재식별 모니터링 (자유양식)	가명정보 이용기간 종료 후 3년간 보관
	가명정보 회수 및 처리 중단	개인정보 재식별된 경우 해당 가명정보 회수, 처리 중단 및 즉시 파기	가명정보 파기 계획 및 결과보고서	기록물 관리에 따른 보유기간 내 보관

부록 2-[표 1] 가명처리 단계별 산출물 및 처리방안 예시

가명정보 내부결합

단계		내용	산출물	처리방안
1	결합 타당성 검증 및 부서간 협의	내부 회의 및 사업 추진 타당성 검토, 가명처리 목적 및 가명처리 대상 개인정보 선정	내부결합 사업계획서 (결합키 생성 방안 등 포함)	기록물 관리에 따른 보유기간 내 보관
2	결합 승인 및 추진	사업 설명자료 작성 및 사업 승인 추진		
3	가명정보 생성 등 결합 준비	개인정보 항목 선정·추출	결합키	결합완료 후 삭제
		가명처리하여 가명정보 구성 (가명처리 단계의 모든 산출물 필요함. 단, 적정성 평가는 7번 및 8번에서 수행함으로 생략 가능)	가명정보 등	관련 산출물별 처리방안 참조
		가명정보 보호대책을 수립(내부관리계획 포함 가능)	내부관리계획	준영구 보관
4	가명정보 전송 및 수신	제공부서는 주관부서로 가명정보를 전송하고 주관부서는 해당 가명정보 수신	가명처리 대상 목록 (또는 정보집합물)	결합완료 후 삭제
5	가명정보 결합	결합키 정보를 기준으로 둘 이상의 가명정보 결합 수행	결합된 가명정보	가명정보 이용 및 보유기간 종료 후 삭제
6	가명정보 검증	특이정보 등 재식별 가능성 발생 시 추가적으로 가명처리 (적정성 검토 위원회 부적정 판단 시 추가 가명처리)	가명처리 수준정의표 (별지 2)	가명정보 이용기간 종료 후 3년간 보관
7	적정성 검토 (위원회 구성)	적정성 검토 위원회 구성(3~7명)안을 포함한 적정성 검토 계획 수립 및 위원회 구성	적정성 검토 계획서(위원회 구성안 포함)	기록물 관리에 따른 보유기간 내 보관
8	적정성 검토 위원회 운영	적정성 검토 결과에 대한 결과보고서 작성	적정성 검토 결과보고서, 적정성 검토 종합결과서	가명정보 이용기간 종료 후 3년간 보관
		적정성 검토 결과 부적정 판정 시 해당 단계로 반송 조치		
9	활용 및 안전한관리	활용 및 가명정보 관리대장 기록·관리	가명정보 관리대장 (별지 5)	준영구 보관
		가명정보 등에 대한 안전성 확보 방안 수립 및 운영 (개인정보처리방침 공개, 내부관리계획 수립 등)	개인정보처리방침	준영구 보관
			내부관리계획	준영구 보관
		가명정보를 처리 시 연 1회 이상 개인정보 재식별 여부 점검 수행	재식별 모니터링 (자유양식)	가명정보 이용기간 종료 후 3년간 보관
		개인정보 재식별된 경우 해당 가명정보 회수, 처리 중단 및 즉시 파기	가명정보 파기 계획 및 결과보고서	기록물 관리에 따른 보유기간 내 보관

부록 2-[표 2] 가명정보 내부결합 단계별 산출물 및 처리방안 예시

익명처리

단계		내용	산출물	처리방안
1 단계	목적 및 대상	익명처리 목적 및 익명처리 대상 개인정보 선정	익명정보 활용계획서	기록물 관리에 따른 보유기간 내 보관
	승인 준비	사업 설명자료 작성, 내부 회의 및 사업 추진 타당성 검토(적합성 검토), 사업 승인 추진		
	정보집합물 구성	개인정보 항목 선정 및 추출하여 정보집합물 구성	정보집합물	익명처리 후 삭제
	관리체계 구축	익명정보 보호대책을 수립 (재식별 시 제한대책 포함 가능)	익명정보 활용계획서내 보호대책 포함	기록물 관리에 따른 보유기간 내 보관
2 단계	익명처리 대상 재선정	정보집합물에서 처리대상 및 대상별 특성을 확인하여 최소한의 항목을 추출	익명처리 대상 목록 (또는 정보집합물)	익명처리 후 삭제
	위험성 검토	익명처리 과정을 확인하여 위험성 요소 검증 및 제거, 개인정보 항목별 위험성 분류 및 위험성 식별(식별가능성 및 복원가능성 중심으로 실시)	익명처리 과정 검토 확인서, 위험성 검토서	익명정보 이용기간 종료 후 3년간 보관
	위험성 검토 결과보고서 작성	항목별 위험성 분류 및 위험성 검토 결과를 고려하여 위험성 검토 결과보고서 작성	위험성 검토 결과보고서(별지 3)	
3 단계	항목분류 및 익명처리 수준 정의	개인정보 항목별 위험성 분류 및 항목별 익명처리 수준 정의	익명처리 수준 정의표(별지 4)	익명정보 이용기간 종료 후 3년간 보관
	익명처리 수행 및 처리 검증	익명처리 수행 (익명처리 과정에서 기타정보가 발생하거나 인식된 경우 기타정보는 추가정보에 준하여 즉시 삭제)	익명정보	기간 종료 후 삭제
			기타정보	즉시 삭제
		특이정보 등 재식별 가능성 확인 시 추가적으로 익명처리 (보완조치 수행 시 익명처리 수준 정의표 수정 반영)	익명처리 결과보고서	익명정보 이용기간 종료 후 3년간 보관
4 단계	적정성 검토 위원회 구성	적정성 검토 위원회 구성안을 포함한 적정성 검토 계획 수립	적정성 검토 계획서(위원회 구성안 포함)	기록물 관리에 따른 보유기간 내 보관
	적정성 검토 지원 요청 (필요시)	전문기관에 적정성 검토 지원 요청	적정성 검토 요청서	익명정보 이용기간 종료 후 3년간 보관
	자료 준비	적정성 검토를 위한 기초자료 준비 및 적정성 검토	(기초자료)	기초자료가 포함된 각 산출물 처리방안 참고
	적정성 검토 위원회 운영	적정성 검토 결과에 대한 결과보고서 작성	적정성 검토 결과보고서 (자유양식)	익명정보 이용기간 종료 후 3년간 보관
		적정성 검토 결과 부적정 판정 시 해당 단계로 반송 조치		
		위원 보안서약서 작성	보안서약서 (자유양식)	기록물 관리에 따른 보유기간 내 보관

단계		내용	산출물	처리방안
5 단계	익명정보 처리 기록·관리	익명정보 관리대장 기록·관리	익명정보 관리대장 (별지 5)	준영구 보관
	익명정보 재식별 시 대응조치 수행	재식별 사고 발생 시 대응계획 및 제3자 제공 시 제한사항이 포함된 계약서	사업계획서 (재식별 사고 대응계획)	기록물 관리에 따른 보유기간 내 보관
			계약서 (해당시)	법령에 따른 보유기간

부록 2-[표-3] 익명처리 단계별 산출물 및 처리방안 예시

※ 위의 가명·익명 처리 및 내부결합에 따른 산출물 및 처리방안은 예시로 제시한 것이며 개인정보처리자별 개인정보 처리 환경 및 상황 등에 따라 변경 활용

※ 서로 다른 개인정보처리자 간의 가명정보의 결합(외부결합)으로 발생하는 산출물은 개인정보보호위원회 또는 관계 중앙행정기관의 장이 지정하는 결합전문기관이 정한 사항을 따름

부록2 가명처리 및 익명처리 관련 양식

[별지 1] 가명정보 식별 위험성 검토 결과보고서 예시

가명정보 식별 위험성 검토 결과보고서(일반형)

<table>
<tr><td>가명정보
활용목적</td><td colspan="2">• AA교육청이 가명처리한 거주지별 학생정보와 성적 정보들을 A기관에 제공하여, 코로나로 원격학습에 따른 지역별 학업 성취도 격차를 파악하기 위한 연구 수행</td></tr>
<tr><td>가명처리
대상
데이터 항목</td><td colspan="2">• 학번, 과목, 학년, 성명, 성적(점수), 시도, 시군구, 읍면동, 지번, 거주지 유형, ㅇㅇㅇ, ㅁㅁㅁ, … (전체 20개의 컬럼)
• AA교육청 내 학생정보 100만명 중에서 B교육지원청과 C교육지원청에 속한 초등학교 및 중학교 학생에 대한 데이터</td></tr>
<tr><td rowspan="3">데이터
식별 위험성</td><td>식별성
유무</td><td>• 교육분야 개인정보 항목별 위험성 목록에 따라,
• 학번, 성명은 개인식별정보임 (중략)
• 위험성 목록에는 없는 ㅁㅁㅁ항목은 위험성 목록 CCC와 유사하므로 이를 준용하여 개인식별정보로 판단하고 위험성은 4로 판단</td></tr>
<tr><td>특이정보
유무</td><td>• 성적 점수의 특성상 최고점과 최하점은 특이정보로 인한 개인 식별성이 발생할 수 있음
• 주소와 거주지 유형(단독주택)에 따른 특이정보로 인한 개인 식별성이 발생할 수 있음</td></tr>
<tr><td>재식별시
영향도</td><td>• 민감한 거주지 유형과 성적 정보로 인한 재식별 발생 시 영향도가 일정 수준 있을 것으로 보임</td></tr>
<tr><td rowspan="3">처리 환경
식별 위험성</td><td>이용 및
제공 형태</td><td>• 교육청 내부 이용</td></tr>
<tr><td>처리 장소</td><td>• 교육청 내 별도 분석 공간을 마련하고 전용 분석 PC에서 사용
• 분석 공간에 대해 엄격한 출입통제 실시 및 관련 출입관리대장 기록·관리
• 분석PC는 인터넷 및 추가정보, 원본정보 및 다른 정보에 접근할 수 없도록 조치하여 분석할 예정임</td></tr>
<tr><td>다른 정보
결합 가능성</td><td>• 가명처리 전 개인정보를 교육청이 보관하고 있음</td></tr>
<tr><td>최종
검토의견*</td><td colspan="2">• 해당 연구는 교육청 내부에서 활용하는 것으로 데이터 자체 위험성과 처리환경 위험성을 고려할 때 다음과 같은 조치가 필요함
- 학번은 그 자체로 또는 결합시 식별될 가능성이 매우 높으므로 반드시 필요하지 않은 경우 삭제하고 그 과목별, 학년별 성적 추적을 위해 필요한 경우 학번을 그대로 사용하지 않도록 가명처리가 필요
- 성적은 결합 시 식별될 가능성이 있고 필요한 경우가 아니면 특정 항목은 삭제가 필요. 다만, 목적 달성에 필요한 경우에 한해 범주화하여 처리
※ 성적은 특이정보 가능성이 높으므로 범주화 등의 가명처리가 필요
- 지번의 경우 다른(공개된 정보 등) 정보를 통해 재식별 가능성이 있어 삭제 또는 목적 달성에 필요한 경우 가명처리 필요
• 그 외의 정보들은 재식별 가능성이 낮으며 목적 달성을 위해 필요하다고 판단되므로 가명처리 하지 않음</td></tr>
<tr><td colspan="3">[별첨] 식별 위험성 검토를 위한 근거 자료(검토서) 1부</td></tr>
</table>

* 최종 검토의견은 외부전문가를 활용하여 자문 및 작성을 요청할 수 있음

가명정보 식별 위험성 검토 결과보고서(체크리스트 이용시)

<table>
<tr><td colspan="3">가명정보 활용목적</td><td>• AA교육청이 가명처리한 거주지별 학생정보와 성적 정보들을 A기관에 제공하여, 코로나로 원격학습에 따른 지역별 학업 성취도 격차를 파악하기 위한 연구 수행</td></tr>
<tr><td colspan="3">가명처리 대상 데이터 항목</td><td>• 학번, 과목, 학년, 성명, 성적(점수), 시도, 시군구, 읍면동, 거주지 유형, 지번, ㅇㅇㅇ,ㅁㅁㅁ, … (전체 20개의 컬럼)
• AA교육청 내 학생정보 100만명 중에서 B교육지원청과 C교육지원청에 속한 초등학교 및 중학교 학생에 대한 데이터</td></tr>
<tr><td colspan="3">이용기관의 개인정보보호수준</td><td>• 보호법 제28조의4(가명정보에 대한 안전조치 의무 등), ….등에 따른 법적 준수사항들을 모두 만족하고 있음</td></tr>
<tr><td rowspan="11">위험성검토</td><td rowspan="3">데이터</td><td>데이터 구성</td><td>• 총 6가지 항목에 대한 위험성 검토 결과 10 기준으로 3 수준으로 나타나 데이터 구성을 통한 식별 가능성은 낮은 편임</td></tr>
<tr><td>데이터 분포</td><td>• 총 2가지 항목에 대한 위험성 검토 결과 10 기준으로 3 수준으로 나타나 데이터 분포를 통한 식별 가능성은 낮은 편임</td></tr>
<tr><td>재식별 영향도</td><td>• 총 2가지 항목에 대한 위험성 검토 결과 10 기준으로 3 수준으로 나타나 재식별 영향도는 낮은 편임</td></tr>
<tr><td rowspan="4">처리환경</td><td>가명정보 처리 장소 및 형태</td><td>• 타 부서에서 자체 가명정보를 처리할 예정이며, 제한구역에서 처리하여 위험성은 10 기준으로 2 수준으로 매우 낮은 편임</td></tr>
<tr><td>다른정보 보유여부</td><td>• 총 5가지 항목에 대한 위험성 검토 결과 10 기준으로 2 수준으로 나타나 다른 정보와의 결합을 통한 식별 가능성은 매우 낮은 편임
※ 위탁 또는 제3자 제공하는 경우는 3가지 항목 해당(p.89 참고)</td></tr>
<tr><td>이용기관의 신뢰도</td><td>• 총 6가지 항목에 대한 위험성 검토 결과 10 기준으로 2 수준으로 나타나 이용기관의 신뢰도는 높은 편임</td></tr>
<tr><td>우연한 재식별</td><td>• 총 4가지 항목에 대한 위험성 검토 결과 10 기준으로 3 수준으로 나타나 우연한 재식별 가능성은 낮은 편임</td></tr>
<tr><td rowspan="4">경감</td><td>가명.익명처리*</td><td>• 해당사항 없음(수준 정의표에서 반영할 예정)</td></tr>
<tr><td>장소 통제 강화</td><td>• 안전구역(통제구역보다 강력한 통제 실시) 설정 및 해당 구역에서 가명정보 처리를 실시하여 총점에서 경감 -2점 실시</td></tr>
<tr><td>인원 통제 강화
인증 등 신뢰도
기타</td><td>• 해당사항 없음</td></tr>
<tr><td colspan="2">종합 검토 결과</td><td>• 식별 위험성에 대한 종합 검토 결과, 이용기관의 개인정보보호능력을 제외한 총 6가지 항목들에 대해 종합 위험성 점수는 80 기준으로 16 수준으로 나타나 전반적인 위험성은 약간 낮은 편임</td></tr>
<tr><td colspan="3">최종 검토 의견</td><td>• 해당 연구는 교육청 내부에서 활용하는 것으로 데이터 자체 위험성과 처리환경 위험성을 고려할 때 다음과 같은 조치가 필요함
- 학번은 그 자체로 또는 결합시 식별될 가능성이 매우 높으므로 반드시 필요하지 않은 경우 삭제하고 그 과목별, 학년별 성적 추적을 위해 필요한 경우 학번을 그대로 사용하지 않도록 가명처리가 필요
- 성적은 결합시 식별될 가능성이 있고 필요한 경우가 아니면 특정 항목은 삭제가 필요.(성적은 특이정보 가능성이 높아 가명처리 필요)
- 지번의 경우 다른(공개된 정보 등) 정보를 통해 재식별 가능성이 있어 삭제 또는 목적달성에 필요한 경우 가명처리 필요
- …..
• 그 외의 정보들은 재식별 가능성이 낮으며 목적 달성을 위해 필요하다고 판단되므로 가명처리 하지 않음</td></tr>
<tr><td colspan="4">[별첨] 식별 위험성 검토를 위한 근거 자료(체크리스트) 1부</td></tr>
</table>

[별지 2] 가명처리 수준 정의표 예시

‘가명정보 식별 위험성 검토 결과보고서’에 분류한 개인정보에 대한 가명처리 수준 정의

순번	항목명	처리기술 및 수준	기타
1	학생개인번호	◦ 가명처리 (암호화 : SHA2 + Salt)	◦ 학년별, 과목별 추적 분석 등을 위해 가명처리 수행
2	과목	◦ 처리하지 않음	◦ 처리하지 않는 항목을 작성 (과목, 성별 등이 결합하여 특이정보가 발생할 경우 삭제 등의 가명처리 필요)
3	학년		
4	성별		
5	성적(점수)	◦ 가명처리 (범주화 : 100점 만점 기준으로 2~5점 단위)	◦ 특이정보 발생시 범주화 기준 상향 필요
6	시도	◦ 처리하지 않음 (항목이 다수여서 작성이 어려운 경우 ‘별지’를 활용하여 목록만 제시)	◦ 처리하지 않는 항목을 작성
7	시군구		
8	읍면동		
9	거주지 유형		
10	지번	◦ 가명처리(삭제)	◦ 세부 지번의 정보는 분석 목적에 필요하지 않음

[별지 3] 익명정보 식별 위험성 검토 결과보고서 예시

익명정보 활용목적		◦ ○○교육청은 익명처리한 학생의 과목, 학년, 성별, 성적을 학부모에게 공개하여 과목별·학년별·성별 성적 분포도를 제공하고자 함
익명정보 항목		◦ 학번, 과목, 학년, 성별, 성적(점수), 시도, 시군구, 읍면동, 거주지 유형, 지번 ※ 항목을 나열하지 못하는 경우 '별지'로 추가하여 사용 가능
처리(제공) 환경 검토	처리 환경	◦ 단일목적인 경우로 위험성은 낮으나 외부 불특정 다수에 일반 공개로 전체적인 위험성은 매우 높은 편임
	제공받는 자의 개인정보 보호수준	◦ 법령에서 요구하는 개인정보 안전조치 기준의 최소 요건보다 매우 높은 수준으로 위험성은 매우 낮은 편임
	재식별 가능성	◦ 불특정 다수인 학부모를 대상으로 공개되는 환경으로 특정인을 한정할 수 없기에 재식별에 대한 시도 가능성은 매우 높은 편임
	재식별시 정보주체에게 미치는 영향	◦ 학부모에게 공개되는 정보는 익명처리된 성적 분포도로 재식별 될 경우 정보주체인 학생의 프라이버시를 침해하거나 경제적·비경제적 손실을 발생시킬 가능성은 보통 수준임
항목별 위험성 분석		◦ 학번 및 지번은 개인을 명확하게 알아볼 수 있음 ◦ 학년, 과목, 성별, 성적의 결합은 특성 집합을 관찰하여 개인을 알아볼 가능성이 존재 ◦ 특정 과목, 특이 성적의 결합은 무시할 수 없는 확률로 추론하여 개인을 알아볼 가능성 존재 ◦ 모든 항목들의 일반화가 부족할 경우 외부 공개된 정보와 연결하여 개인을 알아볼 가능성이 존재
최종 검토의견*		◦ 해당 정보는 불특정 다수에게 제공하는 외부 공개에 해당하며, 제공받는 자가 별도의 다른 (개인)정보를 통해 가명정보 재식별을 시도할 가능성이 매우 높음 ◦ 처리환경은 매우 높음, 제공받는 자의 개인정보 보호수준은 매우 낮음, 재식별 가능성은 매우 높음, 재식별시 정보주체에게 미치는 영향은 보통임 ◦ 따라서, 전체적인 위험성은 매우 높음으로 측정됨 ◦ 과목, 학년, 성별, 성적 결합시 특이정보에 따라 식별될 가능성이 높으므로 반드시 일반화의 강도를 높여서 처리해야 함. 최소한 k-익명성(k=50) 적용하여 처리 ※ '성적(점수)'는 특이정보 가능성이 존재하므로 범주화 등의 익명처리가 필요 ※ '과목'은 특이정보 가능성이 존재하므로 익명처리가 필요 ◦ '학번', '시도', ' 시군구', '읍면동', '거주지 유형', '지번'의 경우 다른(공개된 정보 등) 정보를 통해 재식별 가능성이 높고 목적 달성에 불필요하므로 삭제 필요

* 최종 검토의견은 외부전문가를 활용하여 자문 및 작성을 요청할 수 있음

[별지 4] 익명처리 수준 정의표 예시

‘익명정보 식별 위험성 검토 결과보고서’에 분류한 개인정보에 대한 익명처리 수준 정의

• ○○교육청 과목별·학년별·성별 성적 현황

순번	항목명	속성	처리 기술 및 수준	기타
1	학생개인번호	개인식별정보	◦ 익명처리(삭제)	◦ 학생개인번호 정보는 분석 목적에 필요하지 않음
2	과목	개인식별가능정보 (k-익명성 적용)	◦ 익명처리(범주화)	◦ 처리하지 않는 항목을 작성 (과목, 성별 등이 결합하여 특이정보가 발생할 경우 삭제 등의 가명처리 필요)
3	학년			
4	성별			
5	성적(점수)	개인식별가능정보 (k-익명성 미적용)	◦ 익명처리 (일반화 : 100점 만점 기준으로 5점 단위, 60점 미만 삭제 및 95점 이상은 90~100점으로 일반화)	◦ 특이정보 발생시 일반화 기준 상향 필요
6	시도	개인식별가능정보	◦ 익명처리(삭제)	◦ 해당 정보는 분석 목적에 필요하지 않음
7	시군구			
8	읍면동			
9	거주지 유형			
10	지번			

※ 익명처리 결과 k-익명성의 k값은 기관의 내부 기준에 따라 값을 산정

[별지 5] 가명정보 관리대장

여러 건을 작성할 수 있도록 하는 복수 가로형 또는 건별 작성을 위한 단수 세로형을 기관의 특성에 따라 선택적으로 기록관리할 수 있음

복수 가로형 가명정보 관리대장

순번	기간	목적	항목	처리 및 보유기간	제공 받는 자 등	위탁 사항	제한 사항	처리 구분	기타 (추가정보)	가명처리 수행자	책임자

1. 순번 : 가명정보 처리에 대한 순서를 작성한다.
2. 기간 : 가명처리를 시작한 날부터 끝난 날까지의 기간을 작성한다.
3. 목적 : 가명정보를 처리하는 목적을 작성한다.
4. 항목 : 처리하는 가명정보의 항목을 작성한다.
5. 처리 및 보유기간 (필요시) : 가명정보의 사용 및 보유기간을 작성한다.
   ※ 예시) 처리기간(2년), 보유기간(1년) or 처리기간(1년), 보유기간(없음) 등
6. 제공받는 자 등 : 제3자 제공시 제공받는 자의 정보를 작성한다.
   내부결합하는 경우 결합대상 부서명을 작성한다.
   가명정보 결합시 결합대상 가명정보처리자의 정보를 작성한다.
7. 위탁사항 : 가명정보 처리를 위탁한 경우 해당 사항을 작성한다.
8. 제한사항 : 가명정보 처리 유형에 따라 제한사항을 둔 내용을 작성한다.
9. 처리구분 : 가명정보 처리 유형을 작성한다. 예시) 생성, 결합, 제공, 공개 등
10. 기타(추가정보) : 추가정보는 가명정보 생성 즉시 파기 후 '추가정보 동시 파기'로 작성하고 추가정보를 보관해야 하는 경우 최종적인 사용이 끝나고 추가정보를 파기하는 경우에 파기날짜를 기재한다. 내부결합을 하는 경우 제공하는 부서는 가명정보 및 추가정보 모두를 삭제하고 '가명정보 및 추가정보 파기'로 작성한다.
11. 가명처리를 수행한 자 : 가명처리를 수행한 자의 이름을 작성하고 서명한다.
12. 책임자 : 가명정보 처리 책임자 이름을 작성하고 서명한다. (ex. 가명처리 부서의 책임자)

단수 세로형 가명정보 관리대장

구분	내용	비고
기간		
목적		
항목		
처리 및 보유기간		
제공받는 자		
위탁사항		
제한사항		
처리 구분		
기타 (추가정보)		
가명처리 수행자		
책임자		

[별지 6] 익명정보 관리대장

여러 건을 작성할 수 있도록 하는 복수 가로형 또는 건별 작성을 위한 단수 세로형을 기관의 특성에 따라 선택적으로 기록관리할 수 있음

복수 가로형 익명정보 관리대장

순번	기간	항목	사유/근거	제공받은 자	제한사항	기타	익명처리 수행자	책임자

1. 순번 : 익명정보 처리내용에 대한 순서를 작성한다.
2. 기간 : 익명처리를 시작한 날부터 끝난 날까지의 기간을 작성한다.
3. 항목 : 익명정보의 항목을 작성한다.
4. 사유/근거 : 익명정보 처리 사유 및 근거를 작성한다.
5. 제공받은 자 : 익명정보를 제공한 경우 제공받은 자의 정보를 작성한다.
   ※ 예시) 기업명 또는 성명, 담당자 연락처
6. 제한사항 : 익명정보 처리 유형에 따라 제한사항을 둔 내용을 작성한다.
   ※ 예시) ①처리기간(2년), 보유기간(1년) or 처리기간(1년), 보유기간(없음), ②제3자 제공시 계약서 준수 여부 등
7. 기타 : 익명정보 재식별시 파기 여부 등 추가적으로 필요한 내용을 작성한다.
8. 익명처리를 수행한 자 : 익명처리를 수행한 자의 이름을 작성하고 서명한다.
9. 책임자 : 익명처리 책임자의 이름을 작성하고 서명한다.

단수 세로형 익명정보 관리대장

구분	내용	비고
기간		
항목		
사유 / 근거		
제공받은 자		
제한사항		
기타		
익명처리 수행자		
책임자		

[별지 7] 가명처리 계획서 및 가명정보 결합신청서

아래의 가명처리 계획서 요약본 양식은 예시이며 기관의 특성을 반영하여 가공하여 적용할 수 있음

통계작성 계획서 양식

통계작성 계획서		
통계명		
대표 참여진	소속	
	담당자명	
통계작성 배경 및 목적		
통계작성 대상자 수		
통계작성 계획 및 방법		
기대효과 및 활용방안		
붙임 상세 통계작성 계획서 - 가명처리 과정 위험성 판단 관련 자료 - 제공받는 제3자의 개인정보 보호수준 관련 자료 등을 포함해야 함		

과학적 연구 계획서 양식

과학적 연구 계획서		
연구명		
연구진	소속	
	연구책임자	
연구 배경 및 목적		
예상 연구 기간		
연구 대상자 수		
연구 방법		
연구내용		
기대효과 및 활용방안		
붙임. 상세 연구계획서 등 - 가명처리 과정 위험성 판단 관련 자료 - 제공받는 제3자의 개인정보 보호수준 관련 자료 등을 포함해야 함		

공익적 기록보존 계획서 예시

<table>
<tr><th colspan="3">공익적 기록보존 계획서</th></tr>
<tr><td>공익적 기록보존명</td><td colspan="2"></td></tr>
<tr><td rowspan="2">대표 참여진
(기록보관 기관)</td><td>보관기관명</td><td></td></tr>
<tr><td>담당자명</td><td></td></tr>
<tr><td>공익적 기록보존
목적</td><td colspan="2"></td></tr>
<tr><td>보존기간</td><td colspan="2"></td></tr>
<tr><td>공익적 기록보존
방법</td><td colspan="2"></td></tr>
<tr><td>내용</td><td colspan="2"></td></tr>
<tr><td>기대효과 및
활용방안</td><td colspan="2"></td></tr>
<tr><td colspan="3">붙임. 상세 계획서 등
- 가명처리 과정 위험성 판단 관련 자료
- 제공받는 제3자의 개인정보 보호수준 관련 자료 등을 포함해야 함</td></tr>
</table>

가명정보 결합 신청서

① 결합신청서

② 신청번호 / 접수번호

☐ 가명정보 제공 ☐ 가명정보 제공+결합정보 이용 ☐ 결합정보 이용

결합신청자			
기관명	*A사*	사업자등록번호 또는 법인등록번호	*000-00-00000*
주소	*00시 00구 000*	대표자명	*000*
담당자	*홍길동*	담당자 연락처 (전화, e-mail)	*010-0000-0000* *ooooo@ooooo.oo.oo*
유형	[ ] 개인 [∨] 공공기관 [ ] 비영리법인 [ ] 민간기관		

결합 개요	
③ 반복결합	[∨] 해당없음 [ ] 최초 [ ] 추가(결합접수번호 :)
④ 추가절차 신청	결합률 확인 [∨] 가명정보 추출 [∨] 모의결합 [ ]

⑤ 가명정보 제공자	해당없음 [ ]
파일명	*abc*
제출 방법	[∨] 온라인 [ ] 오프라인
제출 예정일	*0000*년 *00*월 *00*일
제공정보 요약	파일 크기(*0.0GB*) 전체 레코드 수(*000,000개*) 모의결합 레코드 수(*000개*)
전체 가명정보 제공자명(총수)	*총 2개 : A사(파일명 : abc), B사(파일명 : zyx)*
지원 요청 사항	[∨] 결합 신청에 필요한 가명처리

⑥ 결합정보 이용자	해당없음 [ ]
결합 목적	[ ] 통계작성 [∨] 과학적 연구 [ ] 공익적 기록보존 등
세부 결합 목적	*구체적 목적 설명*
분석공간 이용	[ ] 추가 가명처리만 수행 [∨] 결합정보 분석 [ ] 이용안함
지원 요청 사항	[∨] 반출 전 처리 [∨] 분석

「개인정보 보호법」 제28조의3제1항 및 같은 법 시행령 제29조의3제1항에 따른 결합을 위하여 결합전문기관에 결합신청서를 위와 같이 제출합니다.

*0000*년 *00*월 *00*일

결합신청자 *홍길동* (서명 또는 인)

결합전문기관의 장 귀하

⑦ 첨부 서류
1. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류 1부 2. 결합 목적을 증명할 수 있는 서류 1부(결합된 정보를 반출하려는 자에 한함) 3. 결합 대상 가명정보에 관한 서류(전체 항목명, 가명처리 대상 항목명*, 가명처리 내역 등**) 1부(가명정보 제공자에 한함) * 결합키 생성에 사용된 항목 제외 ** 결합 대상 정보가 확정된 이후에 제출

① 결합신청서 작성

○ (작성 주체) 결합신청서는 결합신청자*별로 각자 제출하는 것이 원칙

* 가명정보를 보유하고 있는 개인정보처리자, 현재 가명정보를 보유하고 있지 않으나 결합된 가명정보를 처리할 예정인 개인정보처리자

- 작성자가 해당되는 결합신청자의 유형(가명정보 제공, 가명정보 제공 및 결합정보 이용, 결합정보 이용) 표기

② 신청번호 및 접수번호

○ (신청번호) 결합신청자 중 대표자*가 결합종합지원시스템(link.privacy.go.kr)을 통해 발급받은 번호

* 결합신청에 있어 총괄 관리·감독을 수행할 결합신청자

○ (접수번호) 결합전문기관이 제출된 결합신청서를 접수할 때 발행하는 번호, 결합신청서 제출 시 공란으로 제출

③ 반복결합

○ 추후 동일한 목적·형태 등으로 주기적·반복적 결합을 수행하는 경우

- (최초) 반복결합을 최초로 신청하는 경우
- (추가) 최초 반복결합이 완료된 이후 반복결합을 추가로 신청한 경우, 최초 반복결합 신청시 발급되었던 접수번호 기재

④ 추가절차 신청

○ 결합률 확인, 추출, 모의결합*을 신청하는 자는 해당 사항을 체크(중복체크 가능, 선택사항)

* 모의결합의 경우 결합전문기관별로 지원여부가 다르므로 신청하려는 결합전문기관이 모의결합을 지원하는지 여부를 확인한 후 신청 필요

⑤ 가명정보 제공자(개인정보처리자)

○ 결합을 위해 가명정보를 결합전문기관에 제공하는 자가 작성하며, 가명정보를 보유하고 있지 않은 자는 해당없음에 체크하고 나머지 항목은 공란

- 가명정보 파일명, 제출 방법, 제공 정보 요약, 전체 가명정보 제공자명(총수)*, 지원 요청 사항** 등 작성

* 해당 결합을 신청하는 가명정보 제공자의 전체 기관명 및 전체 기관수(총 0개)

** 가명처리를 직접 수행하기 어려운 가명정보 제공자는 결합전문기관에 결합 전 가명처리의 지원을 요청할 수 있음(이 경우 해당 결합전문기관의 지원여부 확인 필요)

⑥ 결합정보 이용자(개인정보처리자)

○ 결합된 정보를 이용하려는 자(현재 가명정보를 보유하고 있지 않은 자 포함)가 작성하며, 가명정보를 제공하나 결합된 정보를 이용하지 않는 자는 해당없음에 체크하고 공란

- 결합 목적, 분석공간 이용여부*, 지원 요청 사항(중복체크 가능)** 작성

* 결합된 정보를 결합전문기관이 제공하는 인프라를 활용하여 추가 가명처리 및 분석을 하고자 하는 경우(선택 사항) 체크

** 결합전문기관에 결합된 정보에 대한 반출 전 가명·익명처리, 결합된 정보 분석을 요청하고자 하는 자는 해당 지원 사항란 표시(이 경우 해당 결합전문기관의 지원여부 확인 필요)

⑦ 첨부 서류

○ 각 첨부 서류별 제출 주체는 아래와 같으며, 가명정보를 제공하는 자가 결합된 정보도 처리하고자 하는 경우에는 모든 첨부 서류 제출 필요

- 첨부 서류는 결합신청 시 제출하는 것이 원칙이나 결합전문기관과 협의를 통해 결합률 확인, 가명정보 추출 등 모든 사전절차가 완료되어 결합 대상이 확정된 이후 결합 대상 가명정보에 관한 서류를 제출할 수 있도록 협의 가능

구비 서류	가명정보 제공자	결합정보 이용자
1. 결합신청자 관련 서류	○	○
2 결합 목적 관련 서류		○
3. 결합 대상 가명정보에 관한 서류	○	

가명정보 반출 신청서

① 반출신청서

②

반출접수번호	
결합접수번호	

결합신청자			
기관명	*A사*	사업자등록번호 또는 법인등록번호	*000-00-00000*
주소	*00시 00구 000*	대표자명	*000*
담당자	*홍길동*	담당자 연락처 (전화, e-mail)	*010-0000-0000* *ooooo@ooooo.oo.oo*

③ 결합 유형		
반복결합	[ ] 최초	[ ] 추가

④ 반출 개요			
파일명	*ccdab*		
반출 목적	[ ] 통계작성	[∨] 과학적 연구	[ ] 공익적 기록보존 등
세부 반출 목적	*구체적 목적 설명*		
반출 정보 유형	[∨] 가명정보	[ ] 법 제58조의2에 해당하는 정보(익명정보)	
제공 받는 방법	[∨] 온라인	[ ] 오프라인	[ ] 결합전문기관 내 분석공간
지원 요청 사항	[∨] 반출된 정보의 분석	[∨] 개인정보 보호 교육	

「개인정보 보호법」 제28조의3제2항 및 같은 법 시행령 제29조의3제3항·제6항, 「가명정보의 결합 및 반출 등에 관한 고시」 제10조제3항에 따라 결합된 정보를 반출하기 위하여 결합전문기관에 반출신청서를 위와 같이 제출합니다.

*0000*년 *00*월 *00*일

결합신청자 *홍길동* (서명 또는 인)

결합전문기관의 장 귀하

⑤ 첨부 서류	
	1. 반출 대상 정보에 관한 서류 1부(추가적인 서류 제출이 필요한 경우에 한함)
	2. 반출 목적을 증명할 수 있는 서류 1부(추가적인 서류 제출이 필요한 경우에 한함)
	3. 반출 정보의 안전조치계획 및 이를 증빙할 수 있는 서류 1부

① 반출신청서 작성

- (작성 주체) 결합된 정보 또는 분석결과 등을 결합전문기관 외부로 반출하고자 하는 자는 반출신청서를 작성하여 결합전문기관에 제출

※ 가명정보를 제공만 하는 자와 결합된 정보를 결합전문기관 내의 분석공간에서 분석만을 수행하는 자는 반출신청서를 작성하지 않아도 됨

② 반출접수번호 및 결합접수번호

- (반출접수번호) 결합전문기관이 제출된 반출신청서를 접수할 때 발행하는 번호, 반출신청서 제출 시 공란으로 제출
- (결합접수번호) 결합전문기관이 제출된 결합신청서를 접수할 때 발행한 번호

③ 결합 유형

- 반복결합을 신청한 자는 최초·추가 여부를 체크하며, 반복결합이 아닌 경우 공란

④ 반출 개요

- 결합된 정보를 반출하려는 결합신청자는 파일명(반출할 결합 결과물), 반출 목적, 반출정보 유형 등을 작성

※ 결합신청자는 반출심사 전인 경우 결합 목적과 반출 목적 변경 가능

- (반출정보 유형) 반출을 신청하려는 자가 정보의 형태 등을 고려하여 가명 또는 익명으로 판단하여 표기
- (제공받는 방법) 결합전문기관등이 제공하는 시스템을 통해 제공받는 경우는 온라인, USB등 저장장치를 이용해 반출하는 경우는 오프라인, 결합전문기관이 제공하는 분석공간을 이용하는 경우로 구분하여 표기
- (지원 요청사항) 정보의 분석을 위해 결합전문기관의 지원이나 가명정보의 처리에 관한 교육이 필요하면 표기

⑤ 첨부 서류

○ 추가적인 서류 제출이 필요한 경우에 한하여 모든 서류를 제출

- (반출 대상 정보에 관한 서류) 분석공간을 통해 추가 가명처리가 수행되어 반출 대상 정보가 당초 제출한 결합 대상 가명정보와 상이한 경우에만 제출하고 동일한 경우에는 생략 가능
- (반출 목적 관련 서류) 반출 목적이 당초의 결합 목적과 달라진 경우(결합 목적과 반출 목적의 양립 가능성 검토 필요)만 제출하고 동일한 경우에는 생략 가능
- (안전조치 계획) 개인정보 처리방침, 내부관리 계획, 운영 지침 등 반출정보의 안전조치와 관련된 자료를 제출

[별지 8] 가명정보의 안전한 관리를 위한 법제적 요구사항

가명정보의 안전한 관리 관련 법제적 요구사항

항목	내용
개인정보보호법	
제28조의4 (가명정보에 대한 안전조치의무 등)	① 개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다. ② 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.
제28조의5 (가명정보 처리 시 금지의무 등)	① 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다. ② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.
개인정보보호법 시행령	
29조의5 (가명정보 등의 안전성 확보조치 등)	① 개인정보처리자는 법 제28조의4제1항에 따라 가명정보 및 가명정보를 원래의 상태로 복원하기 위한 추가 정보(이하 이 조에서 "추가정보"라 한다)에 대하여 다음 각 호의 안전성 확보 조치를 해야 한다. 1. 제30조 또는 제48조의2에 따른 안전성 확보 조치 2. 가명정보와 추가정보의 분리 보관. 다만, 추가정보가 불필요한 경우에는 추가정보를 파기해야 한다. 3. 가명정보와 추가정보에 대한 접근 권한의 분리. 다만, 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등 접근 권한의 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 접근 권한만 부여하고 접근 권한의 보유 현황을 기록으로 보관하는 등 접근 권한을 관리·통제해야 한다. ② 법 제28조의4제2항에서 "대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다. 1. 가명정보 처리의 목적 2. 가명처리한 개인정보의 항목 3. 가명정보의 이용내역 4. 제3자 제공 시 제공받는 자 5. 그 밖에 가명정보의 처리 내용을 관리하기 위하여 보호위원회가 필요하다고 인정하여 고시하는 사항

항목	내용
제30조 (개인정보의 안전성 확보 조치)	① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다. 1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립ㆍ시행 2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치 3. 개인정보를 안전하게 저장ㆍ전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조ㆍ변조 방지를 위한 조치 5. 개인정보에 대한 보안프로그램의 설치 및 갱신 6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 ② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다. ③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.
개인정보의 안정성 확보조치 기준	
제4조 (내부 관리계획의 수립·시행)	① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립· 시행하여야 한다. 1. 개인정보 보호책임자의 지정에 관한 사항 2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항 3. 개인정보취급자에 대한 교육에 관한 사항 4. 접근 권한의 관리에 관한 사항 5. 접근 통제에 관한 사항 6. 개인정보의 암호화 조치에 관한 사항 7. 접속기록 보관 및 점검에 관한 사항 8. 악성프로그램 등 방지에 관한 사항 9. 물리적 안전조치에 관한 사항 10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항 11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항 12. 위험도 분석 및 대응방안 마련에 관한 사항 13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항 14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항 15. 그 밖에 개인정보 보호를 위하여 필요한 사항 ② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다. ③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다. ④ 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상으로 점검·관리 하여야 한다.

항목	내용
제5조 (접근 권한의 관리)	① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다. ② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다. ③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다. ④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다. ⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다. ⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다. ⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.
제6조 (접근통제)	① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다. 1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한 2. 개인정보처리시스템에 접속한 IP (Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응 ② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다. ③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다. ④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다. ⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다. ⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있다. ⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다. ⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.

항목	내용
제7조 (개인정보의 암호화)	① 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다. ② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다. ③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다. ④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다. 1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과 2. 암호화 미적용시 위험도 분석에 따른 결과 ⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다. ⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다. ⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다. ⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.
제8조 (접속기록의 보관 및 점검)	① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다. ② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다. ③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.
제9조 (악성프로그램 등 방지)	개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다. 1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지 2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시 3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치
제10조 (관리용 단말기의 안전조치)	개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다. 1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 2. 본래 목적 외로 사용되지 않도록 조치 3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

항목	내용
제11조 (물리적 안전조치)	① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다. ② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다. ③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.
제12조 (재해·재난 대비 안전조치	① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다. ② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다. ③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다.

[별지 9] 가명정보 주요 단계별 활동과 법적 근거

- 가이드라인에서 설명하는 내용 중 법적 근거가 없는 활동에 대해 기관 특성상 수행하지 않는다고 해서 법적 책임을 지는 부분은 아니나 정보주체가 맡긴 개인정보를 안전하게 처리하는 측면에서 준수하여 수행하는 것을 권고

단계	세부단계	법적 근거
사전 준비	**목적 설정**	법 제28조의2 제1항
	가명처리 대상 선정, 가명처리 여부 검토	
	가명정보 처리를 위한 안전조치 이행 (내부관리계획, 안전조치, 개인정보처리방침)	법 제29조(안전조치 의무), 법 제28조의4(가명정보에 대한 안전조치의무 등) 등
	필요 서류 작성 및 내부 승인 절차 수행(필요시)	
위험성 검토	대상 선정	
	위험성 검토 (데이터 식별 위험성, 처리환경의 식별 위험성)	
	식별 위험성 검토 결과보고서 작성	
가명 처리	가명처리 방법 및 수준 정의표작성	
	가명처리	
적정성 검토 및 추가 처리	적정성 검토 위원회 구성	
	적정성 검토 위원회 운영 (기초서류 및 위험성 검토 관련 서류 검토)	
	추가 가명처리	
안전한 관리	**가명정보 관리대장 기록 및 보관**	법 제28조의4 제2항, 시행령 제29조의5(가명정보에 대한 안전성 확보 조치) 제2항
	가명정보에 대한 관리적·기술적·물리적안전조치	법 제29조, 시행령 제29조의5(가명정보에 대한 안전성 확보 조치) 제1항
	재식별금지 모니터링	법 제28조의5(가명정보 처리시 금지의무 등) 제1항, 제2항
	가명정보 내부관리계획 수립 및 시행	법 시행령 제29조의5(가명정보에 대한 안전성 확보조치) 제1항 제1호
	수탁자 관리·감독 (가명정보 처리 업무 위탁시)	법 제26조(업무위탁에 따른 개인정보의 처리 제한)
	추가정보 분리 보관, 접근권한의 분리	시행령 제29조의5(가명정보에 대한 안전성 확보 조치) 제1항 제1호, 제3호

[별지 10] 위험성 검토 체크리스트 예시

개인정보 처리과정 관련 체크리스트

가명처리하는 장소는 기관에서 정하는 안전한 장소에 해당하는가?
가명처리하는 장소에는 가명처리 대상 개인정보 등이 승인없이 반출입 될 수 있는 위험이 없는가?
가명처리를 수행하는 자는 사전에 승인을 받아서 처리장소에 출입을 하고, 처리가 완료된 이후에는 승인이 이루어진 후에 자료를 반출하도록 되어 있는가?
상기와 같은 처리환경 부분에 대해 규정·지침·매뉴얼 등으로 정하고 있는가?
가명처리를 수행하는 자는 해당 가명처리 대상의 개인정보 취급 권한이 없는가?
가명처리를 수행하는 자는 적정성 검토를 수행하지 않는가?
가명처리를 수행하는 자는 처리한 가명정보 또는 추가정보 취급 권한이 없는가?
가명처리를 수행하는 자는 가명처리와 관련하여 안전성 확보조치 등에 대한 교육을 받는가?
상기와 같은 권한관리 부분에 대해 규정·지침·매뉴얼 등으로 정하고 있는가?

※ 필수 요건으로 모두 만족 필요

처리기관의 개인정보 보호수준 체크리스트

개인정보 보호 책임자 지정 및 역할, 책임	데이터 이용기관에 개인정보보호 책임자가 임명되어 있음
	개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항을 명시하고 있음
개인정보취급자에 대한 교육	데이터에 접근할 수 있는 인력에 대해 정기적으로 보안 교육을 실시하고 있음
접근권한의 관리	개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하고 있음
	개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하고 있음
	개인정보처리자는 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하고 있음
	개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하고 있음.
	개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하고 있음
	개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하고 있음

접근 통제	개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 기능을 포함한 조치를 하고 있음
	1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한 2. 개인정보처리시스템에 접속한 IP (Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응
	개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하고 있음
	개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하고 있음
	고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하고 있음
	개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하고 있음
	개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 IP주소 등으로 제한하는 접근 제한 등을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용하고 있음
	개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하고 있음
개인정보의 암호화	1. 개인정보처리자는 고유식별정보, 비밀번호, 바이오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하고 있음
	2. 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하고 있음
	3. 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하고 있음
	개인정보처리자는 상기 1, 2, 3에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화를 적용하고 있음
	개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하고 있음
	개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하고 있음

접속기록 보관 및 점검	개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관, 관리하고 있음(5만명 이상의 정보주체에 관하여 개인정보를 처리하거나 고유식별정보 또는 민감정보를 처리하는 개인정보 처리시스템의 경우 2년 이상)
	개인정보처리시스템의 접속기록 등을 월1회 이상 점검하고 있음(개인정보의 다운로드를 발견하는 경우 그 사유를 반드시 확인하고 있음)
	개인정보취급자의 접속기록이 위변조 및 도난분실되지 않도록 해당 접속기록을 안전하게 보관하고 있음
악성프로그램 등 방지	개인정보처리자는 악성프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하고 있으며, 다음 각 사항을 준수하고 있음 1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지 2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시 3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치
관리용 단말기의 안전조치	개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하고 있음 1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치 2. 본래 목적 외로 사용되지 않도록 조치 3. 악성프로그램 감염 방지 등을 위한 보안조치 적용
물리적 안전조치	개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하고 있음
	개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하고 있음
	개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하고 있음(다만, 별도의 개인정보처리 시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있음)
재해 재난 대비 안전조치	개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하고 있음
	개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하고 있음
개인정보의 파기	개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하고 있음 1. 완전파괴(소각·파쇄 등) 2. 전용 소자장비를 이용하여 삭제 3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행
	개인정보처리자가 개인정보의 일부만을 파기하는 경우, 상기 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하고 있음 1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독 2. 상기 1 이외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

개인정보 위탁 시 보호조치	가명정보 처리업무를 외부에 위탁하는 경우, 가명정보도 개인정보에 해당하므로 개인정보보호법 제26조에 따라 위탁업무 수행 목적 외 가명정보의 처리 금지에 관한 사항 등을 포함한 문서를 작성하고 있음
	위탁하는 업무의 내용과 가명정보 처리업무를 위탁받아 처리하는 자를 공개하고 있으며, 업무 위탁으로 인하여 정보주체의 가명정보가 분실·도난·유출·위조·변조·훼손 또는 재식별되지 아니하도록 수탁자를 교육하고, 처리현황 점검 등 수탁자가 가명정보를 안전하게 처리하는지를 감독할 예정임(포함사항 : 재식별 금지, 재제공 또는 재위탁 제한, 재식별 위험 발생 시 통지)
가명정보의 내부 관리계획	가명정보에 대한 다음과 같은 내부관리계획을 수립하고 있음 1. 가명정보 및 추가정보의 관리책임자 지정에 관한 사항 2. 가명정보 및 추가정보의 관리책임자, 가명정보취급자의 역할 및 책임에 관한 사항 3. 추가정보 별도 분리보관 4. 가명정보 및 추가정보의 안전성확보조치에 관한 사항 5. 가명정보처리자의 교육에 관한 사항 6. 가명정보처리 기록작성 및 보관에 관한 사항 7. 가명정보처리 방침 공개에 관한 사항 8. 가명정보의 재식별금지에 관한 사항
	가명정보처리자는 내부 관리계획에서 정한 사항에 중요한 변경이 있는 경우 이를 즉시 반영하여 내부관리계획을 수정·시행하고, 관리책임자는 연 1회 이상 내부 관리계획 이행 실태를 점검·관리하고 있음
가명정보와 추가정보의 분리보관 및 파기	추가 정보와 가명정보는 물리적으로 분리하여 보관하고 있음
	가명정보 또는 추가정보는 이용목적 달성 후 또는 특정 유지 기간 후에 파기하고 있음
가명정보의 기록관리	가명정보를 처리하고자 하는 경우에는 가명정보의 처리목적 등 가명정보의 처리 내용을 관리하기 위한 다음 사항에 대해 기록을 작성하여 보관하고 있음 -가명처리의 목적 -가명처리한 개인정보의 항목 -가명정보의 이용내역 -제3자 제공시 제공받는자 등

※ 필수 요건으로 모두 만족 필요

데이터 구성 관련 체크리스트

데이터의 항목수	활용할 데이터 항목의 양에 따른 다른 데이터와의 연계 가능성이 많은가 ※ 컬럼이 많을수록 위험성은 더 상승함
데이터셋의 통계적 특성	처리 대상 정보가 단일 통계적 속성, 다중 통계적 속성 등 통계적 속성 여부를 가지는가 ※ 다중 속성을 가질수록 위험성은 더 상승함
데이터의 제공 형태	처리 대상 정보는 다음 중 어떤 제공 형태를 가지는가 - 1회 제공, 2~3회 제공, 3회 이상 또는 주기적 제공 ※ 제공 횟수가 많아질수록 위험성은 더 상승함
모집단의 크기 및 샘플 규모	모집단의 크기 및 샘플(처리대상 정보)의 비율은 어떠한가 ※ 모집단 크기는 작을수록, 샘플비율은 높을수록 위험성은 더 상승함
계층적 특징	처리 대상 정보가 계층적인 특징을 가지는가 ※ 가족관계, 특정 부서의 직책관계 등 계층적 관계가 포함된 데이터가 많을수록 위험성이 높음
데이터의 시간적 특성	처리 대상 정보가 보유한 시간적인 특성(단일/다중/연결시간 특성)을 가지는가 ※ 단일, 다중, 연결시간으로 갈수록 위험성은 더 상승함

데이터 분포 관련 체크리스트

분포	연속적인 숫자형 데이터에서 데이터 값의 분포가 양 끝단의 정보(분포 곡선에 따라 한쪽의 정보 포함)가 작은 인원의 정보가 몇 개의 레코드를 포함하는가 - 레코드 개수가 많이 있을수록 위험성이 높음
	일반적인 문자형 데이터(비 연속적인 숫자형 데이터 및 코드형 데이터 포함)에서 특정 값을 가지고 있는 사람이 적은 인원의 분포를 가지고 있는가 - 포함하는 경우 포함 규모에 따라 위험성 증가 (이하 통일)
특이치	개인 식별이 가능한 직업이 포함되어 있는가 (특정 지역의 국회의원 등)
	공개된 데이터와 비교하여 식별 가능성이 높아질 수 있는 정보가 포함되어 있는가 (공개된 정보에서 특정 지역의 인구비가 너무 높은 경우 등)
	전 국민 데이터와 비교할 때 식별가능성이 있는 특이치가 포함되어 있는가 (기네스북 등의 데이터와 비교할 때 키가 매우 작은 사람 등)
	쉽게 개인을 특정할 수 있는 정보가 포함되어 있는가
	두 개 이상의 컬럼의 조합을 통해 개인의 식별가능성이 높아지는 특이치를 포함하는가
	연속적인 이동에 대한 위치정보와 식별가능한 정보가 함께 포함되어 있는가
	이 외에 개인 식별가능성이 높아질 수 있는 특이치가 포함되어 있는가 (값의 유일성으로 인한 식별가능성이 있는 레코드)

우연한 재식별 관련 체크리스트

수집 및 활용 기관 일치	데이터의 수집기관과 분석기관이 동일한지 여부
상태 정보 보유	데이터 이용자는 데이터에 나타난 상태(예, 질병, 장애, 복지대상자, 학생 등)와 관련된 정보 보유 여부
보유한 정보 (데이터베이스)와 결합	데이터 이용자가 보유한 데이터베이스를 이용하여 처리 대상 정보에 포함된 정보 주체(사람)를 고의가 아닌 우연히 식별할 가능성 여부
기타 개인식별가능 정보 조합	데이터 이용자가 개인식별가능정보들의 조합을 통해 우연히 아는 사람을 식별할 가능성 여부

※ 답이 “예”일수록 위험성이 증가

가명정보 처리장소 및 형태 관련 체크리스트

위험성 크기 방향	처리장소	처리 형태	
⇓	안전한 통제구역	내부 부서 이용	
	통제구역	타 부서 이용	
	제한구역	공동연구	
	기타 장소(일반구역 등)	위탁	
		제3자 제공	교육기관
			교육기관 외

다른 정보 관련 체크리스트

원본정보	• 데이터를 이용하는 시점에 가명처리를 하기 전의 원본정보를 보관하는가 - 보관하는 경우 위험성 증가 • 데이터 이용자의 가명처리하기 전의 원본정보에 대한 접근이 기술적으로 제한되는가 - 접근통제 등으로 제한되어 있지 않으면 위험성 증가 • 데이터 이용자의 가명처리 하기 전의 원본정보에 대한 접근에 대한 관리적인 절차가 수립되어 있는가 - 관리적인 절차가 수립되어 있지 않으면 위험성 증가 • 데이터 이용자의 가명처리 하기 전의 원본정보에 대한 접근이 있을 시 이에 대한 기록을 저장·관리하는가 - 원본정보 접근에 대한 기록 관리하지 않으면 위험성 증가

추가정보	• 데이터를 이용하는 시점에 가명처리시 발생한 추가정보가 보관되어 있는가 - 보관하는 경우 위험성 증가 • 데이터 이용자의 추가정보에 대한 접근이 기술적으로 제한되어 있는가 - 접근통제 등으로 제한되어 있지 않으면 위험성 증가 • 데이터 이용자의 추가정보에 대한 접근에 대한 관리적인 절차가 수립되어 있는가 - 관리적인 절차가 수립되어 있지 않으면 위험성 증가 • 데이터 이용자의 추가정보에 대한 접근이 있을시 이에 대한 기록을 저장, 관리하는가 - 추가정보 접근에 대한 기록 관리하지 않으면 위험성 증가
처리기관의 다른 정보	• 데이터를 이용하는 시점에 가명처리된 정보와 결합하여 개인의 식별이 가능한 다른 정보를 보유하고 있는가 - 보관하는 경우 위험성 증가 • 데이터 이용자의 가명처리된 정보와 결합하여 개인의 식별이 가능한 다른 정보에 대한 접근이 기술적으로 제한하고 있는가 - 접근통제 등으로 제한되어 있지 않으면 위험성 증가 • 데이터 이용자의 가명처리된 정보와 결합하여 개인의 식별이 가능한 다른 정보의 접근에 대한 관리적인 절차가 수립되어 있는가 - 관리적인 절차가 수립되어 있지 않으면 위험성 증가 • 데이터 이용자의 가명처리된 정보와 결합하여 개인의 식별이 가능한 다른 정보에 대한 접근이 있을 시 이에 대한 기록을 저장, 관리하는가 - 다른 정보의 접근에 대한 기록 관리하지 않으면 위험성 증가
공개된 정보	• 데이터를 제공받아 이용하는 시점에 가명처리된 정보와 결합하여 개인의 식별이 가능한 공개된 정보(공공데이터 공개, 통계데이터 공개 등)가 존재하는가 - 공개된 정보가 있으면 위험성 증가
보유 경험 및 지식	• 데이터 이용자의 보유 경험과 지식은 어떠한가 - 다음 순서대로 위험성이 증가 . 데이터 이용자는 분석목적과 유사한 분석을 과거에 수행한 경험 또는 이와 관련된 지식을 보유 . 데이터 이용자는 분석목적과 동일한 분석을 과거에 수행한 경험 보유 . 데이터 이용자는 제공받아 이용하는 데이터와 유사한 정보를 다룬 경험 보유 . 데이터 이용자는 제공받아 이용하는 데이터 중 일부 정보를 다룬 경험 보유 . 데이터 이용자는 제공받아 이용하는 데이터와 완전히 동일한 정보를 다룬 경험 보유

※ 위탁 및 제3자 제공의 경우 원본정보 및 추가정보에 대한 접근이 원천적으로 차단되어 있다는 가정하에 “처리기관의 다른 정보”, “공개된 정보”, “보유 경험 및 지식” 항목에 대해서만 위험성을 검토한다.

처리기관의 신뢰도 관련 체크리스트

기관 유형	가명정보를 이용하는 조직의 유형이 교육기관 or 공공기관 or 민간기관인가 - 교육기관 및 공공(위험성 낮음), 민간(위험성 높음)
이익 창출	가명정보 이용으로 인해 재정적 또는 상업적 이익을 획득할 가능성이 있는가 - 이익을 획득할 수 있을 경우 위험성 증가
사회적 인식	데이터 활용으로 인해 비경제적 이익을 얻거나 또는 사회적인 문제를 일으킬 수 있는가 (정치, 여론조작, 사리사욕, 평판 등)
법 위반 공표사실	이용기관 혹은 위탁기관은 최근 3년 이내에 개인정보보호법 제66조에 따른 공표사실이 있는가 - 제61조에 따른 의견제시 및 개선 권고 - 제64조에 따른 시정조치 명령 - 제65조에 따른 고발 또는 징계권고 - 제75조에 따른 과태료 부과의 내용 및 결과 ※ 제65조 및 75조에 따른 공표사실의 경우 다른 항목보다 2배 이상의 위험성 증가
재식별 위험	재식별을 위한 전문성.재정적 능력 보유하고 있는가 - 유사분석경험 유무 및 분석에 대한 전문인력 보유 여부에 따른 위험성 검토 - 주관적 판단으로 재식별을 위한 재정적 능력이 있을 경우 위험성 증가
보안서약서 징구	보안서약서·확약서는 조직 및 개인 등 복합적으로 징구하는가 - 가명·익명처리 관련 보안서약서를 징구한다. · 조직 차원의 확약서 · 개인별 보안서약서 ※ 확약서 및 보안서약서를 누락하는 항목 및 규모에 따라 위험성 증가

재식별 영향도 관련 체크리스트

재식별시 발생되는 문제	데이터 주체 또는 그들이 속한 그룹에 대한 차별 발생 가능성이 있는가
	정치적, 종교적인 이유로 악용될 가능성이 있는가
	정보주체의 프라이버시가 침해될 가능성이 있는가
	제공자의 경제적, 비경제적 손실*을 발생할 가능성이 있는가 * 정보주체의 이미지 실추, 개인정보 도용으로 인한 범죄 이용 등
처리 대상 정보의 민감성	처리 대상 정보에 민감한 항목들을 포함하는가 (예 : AIDS, 한센병, 고아, 장애인 등)
	처리 대상 데이터의 정보주체가 취약계층에 대한 정보를 포함하는가
	처리 대상 데이터의 정보주체가 사회적인 영향이 매우 큰 사람을 포함하는가 (예 : 정치인, 대통령, 기업총수, 연예등, 종교지도자 등)

※ 가능성이 높을수록 그리고 포함 규모가 클수록 위험성이 증가

[별지 11] 내부관리계획 및 개인정보 처리방침 예시

내부관리계획 예시

제00조(가명정보 및 추가정보 관리책임자 지정) ① ○○○○○(개인정보처리자명)는 가명정보 대한 총괄 관리책임자로 ○○○○○(가명정보 관리책임자명 또는 직책)로 정한다.

② 가명정보 관리책임자는 다음과 같은 역할을 수행한다.

1. 가명정보에 대한 내부 관리계획의 수립·시행
2. 내부 관리계획의 이행실태 점검 및 관리
3. 가명처리 및 적정성 검토 현황 관리
4. 가명정보 및 추가정보에 대한 관리·감독
5. 가명정보 처리 현황 및 관련 기록 관리
6. 가명정보를 처리하는 자 교육계획의 수립 및 시행
7. 가명처리 및 가명정보 처리 위탁 사항에 대한 관리·감독(해당 시)
8. 가명정보에 대한 재식별 모니터링 및 재식별 시 처리 방안의 수립·시행
9. 그 밖의 가명정보 처리에 대한 보호에 관한 사항

제00조(가명정보 및 추가정보의 분리보관) ① 가명정보는 가명처리가 완료되면 가명처리 전 개인정보와 분리·보관하여야 한다.

② 가명처리의 과정에서 발생하는 추가정보는 가명정보와 분리·보관하여야 한다.

③ 가명처리 전 개인정보, 가명정보 및 추가정보는 물리적으로 분리 보관하는 것을 원칙으로 하며 물리적 보관이 어려운 경우 논리적인 분리를 시행할 수 있다.

④ 논리적으로 분리·보관하는 경우 엄격한 접근통제를 적용해야 한다.

제00조(가명정보 및 추가정보에 대한 접근권한 분리) ① 가명처리가 완료되면 가명정보 또는 추가정보의 접근권한은 최소한의 인원으로 엄격하게 통제하여야 하며, 업무에 따라 차등적으로 부여 하여야 한다.

② 추가정보에 대한 접근권한과 가명정보에 대한 접근권한은 분리하여 관리해야 한다.

③ 가명정보 또는 추가정보에 대한 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하도록 하고 이 기록은 최소 3년간 보관하여야 한다.

제00조(가명정보 및 추가정보의 안전성 확보조치) ① 가명정보와 추가정보는 개인정보 보호법 및 동법 시행령에서 요구하는 안전성 확보조치를 수행하여야 한다.

② 추가정보에 특별한 이유가 없는 한 생성 즉시 삭제하도록 한다. 단, 시계열 분석 등의 이유로 추가정보가 필요한 경우 저장 시 암호화하여 저장하여야 한다.

제00조(가명정보를 처리하는 자의 교육) ① 가명정보 관리책임자는 가명정보를 처리하는 자에게 필요한 가명정보 보호 교육계획을 수립하고 실시하여야 한다.

② 가명정보 보호 교육은 다음과 같은 내용을 포함하여 시행하여야 한다.

1. 가명정보 처리 근거에 관한 사항
2. 가명정보 및 추가정보의 안전조치에 관한 사항
3. 재식별 금지에 관한 사항

③ 가명정보를 처리하는 자에 대한 교육은 개인정보 보호교육과 함께 수행할 수 있으며 교육을 실시한 결과 또는 이를 입증할 수 있는 관련 자료 등을 기록·보관하여야 한다.

제00조(가명정보 처리 기록 작성 및 보관) ① 가명정보의 처리 시 다음과 같은 사항에 대해 가명정보 처리 대장에 기록을 작성하여 보관하여야 한다.

1. 가명정보의 처리 목적
2. 가명처리한 개인정보의 항목
3. 가명정보의 이용내역
4. 제3자 제공 시 제공받는 자
5. 그 밖에 가명정보의 처리 내용을 관리하기 위하여 개인정보보호위원회가 필요하다고 인정하여 고시하는 사항

제00조(개인정보 처리방침 공개) ① 가명정보 처리와 관련하여 아래와 같은 내용을 개인정보 처리방침에 포함하여 공개하여야 한다.

1. 가명정보의 처리 목적
2. 가명정보 처리기간(선택)
3. 가명정보 제3자 제공에 관한 사항(해당 시)
4. 가명정보 처리 위탁에 관한 사항(해당 시)
5. 처리하는 가명정보의 항목
6. 가명정보의 안전성 확보조치에 관한 사항

제00조(가명정보의 재식별 금지 등 오남용 제한 및 처벌) ① 가명정보를 처리하는 자의 가명정보에 대한 재식별 등 처리 목적 및 처리 범위 등을 넘어서 오남용하는 행위는 엄격하게 금지한다.

② 가명정보를 처리하는 자가 가명정보를 처리하는 중 특정 개인에 대한 재식별이 발생하는 경우 즉시 처리를 중단하고 이를 가명정보 관리책임자에게 통보한 후 수립된 재식별 시 처리 방안에 따라 즉시 조치하여야 한다.

③ 가명정보의 오남용에 대한 위반행위에 대해서는 ○○○ 위반행위에 준하여 처벌한다.

개인정보 처리방침 예시

제00조(가명정보의 처리)

① OOO(개인정보처리자명)는 수집한 개인정보를 특정 개인을 알아볼 수 없도록 가명처리하여 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 처리할 수 있습니다. 가명정보 처리의 위탁 및 제3자 제공은 하지 않으며, 가명정보는 재식별 되지 않도록 분리하여 별도 저장·관리하고 가명정보의 처리 내용에 대해 기록을 작성하여 보관하는 등 필요한 기술적·관리적 보호조치를 취합니다.

구분	수집·이용 목적	처리항목	보유 및 이용기간
△△△ 연구	연령대별 △△ 등 분석	휴대전화번호, △△일시, △△유형	결합데이터 분석 완료시까지

[별지 12] 개인정보 가명처리 적정성 검토 양식

※ 아래 참고자료는 적정성 검토 시 필요한 사항들에 대한 이해를 돕기 위해 작성한 자료로써 표준이 아니며, 자체적으로 제작하여 다른 자료로 활용할 수 있음

적정성 검토 기초자료 목록 구성표

<table>
<tr><td colspan="3">1. 가명정보 이용·제공 신청서 및 첨부 서류</td></tr>
<tr><td colspan="3">2. 개인정보 유형 분류표</td></tr>
<tr><td colspan="3">3. 가명정보 식별 위험성 검토 결과보고서
※ 가명정보에 대한 안전조치 이행 확약서 포함(이용기관 보호수준 관련)</td></tr>
<tr><td colspan="3">4. 가명처리 방법 및 수준 정의표</td></tr>
<tr><td colspan="3">5. 기초자료명세</td></tr>
<tr><td></td><td rowspan="4">5.1 데이터 명세</td><td>데이터 특징</td></tr>
<tr><td></td><td>데이터 생성 방법</td></tr>
<tr><td></td><td>데이터 제공방법</td></tr>
<tr><td></td><td>데이터 관리 환경</td></tr>
<tr><td></td><td colspan="2">5.2 원본 데이터 세부 항목별 명세 예시</td></tr>
<tr><td></td><td colspan="2">5.3 원본 데이터 예시</td></tr>
<tr><td></td><td colspan="2">5.4 원본 데이터 분포*</td></tr>
<tr><td></td><td colspan="2">5.5 가명처리된 데이터의 세부항목별 명세*</td></tr>
<tr><td></td><td colspan="2">5.6 가명처리된 데이터 예시*</td></tr>
<tr><td></td><td colspan="2">5.7 가명처리된 데이터 분포*</td></tr>
<tr><td colspan="3">6. 가명정보 안전조치 이행 확약서(신청기관용)</td></tr>
</table>

* 데이터 구성 및 가명처리에 따라 변경되는 부분으로 가이드라인에서는 별도 양식을 제시하지 않음

적정성 검토 위원회 운영 세부 양식

1. 적정성 검토 결과서(위원용)
2. 적정성 검토 종합결과서
3. 비밀유지의무 서약서
4. 이해상충 공개 서약서

적정성 검토 기초자료 목록 구성표 세부 양식

1. 가명정보 이용제공 신청서 및 첨부 서류

가명정보 이용·제공 신청서

접수번호		접수일	

신청자	조직/부서명			
	담당자 직위		담당자 성명	
	전화번호		이메일 주소	

처리 목적		☐ 통계작성 ☐ 과학적 연구 ☐ 공익적 기록보존
		세부내용 : *ex) 신용카드 연체와 지방세 연체와의 연관관계 분석 연구*
이용 방법		☐ 내부이용 ☐ 위탁 ☐ 제3자 제공 ☐ 결합전문기관을 통한 결합
이용 주체		☐ 동일 개인정보처리자 ☐ 제3자(제공받는 자) 제공
처리 장소		☐ 내부 ☐ 외부
반복 제공 여부		☐ 1회 제공 ☐ 시계열 분석 등을 위한 반복 제공(회 예정)
제공 방법		☐ 온라인 ☐ 오프라인 ☐ 결합전문기관
신청 명세	가명처리 대상 명칭	*ex) 00시 세금납부 정보*
	데이터 내역	*ex) 최근3년간~~~*
	가명정보 이용 기간	20xx년 xx월 xx일 ~ 20xx년 xx월 xx일

위와 같이 가명정보 이용·제공을 신청합니다.

년 월 일

신청인(부서장명) (서명 또는 인)

첨부서류	1. 요청 정보 상세 내역 2. 활용데이터 요구 수준표(선택) 3. 데이터 처리 위탁 계약서(위탁 계약의 경우) / 추후 제출 4. 데이터 제공 계약서(제3자 제공의 경우) / 추후 제출

2. 개인정보 유형 분류표 및 활용데이터 요구 수준표

개인정보 유형 분류표			
순번	항목명	개인정보유형	비고
1		개인식별정보/ 개인식별가능정보	민감성정보 / 비민감성정보 등
2			
3			
4			
5			

활용 데이터 요구 수준표			
순번	항목명	요구수준	비고
1			
2			
3			
4			
5			

3. 위험성 검토 결과보고서

가명정보 식별 위험성 검토 결과보고서(일반형)

<table>
<tr><td>가명정보
활용목적</td><td colspan="2">• AA교육청이 가명처리한 거주지별 학생정보와 성적 정보들을 A기관에 제공하여, 코로나로 원격학습에 따른 지역별 학업 성취도 격차를 파악하기 위한 연구 수행</td></tr>
<tr><td>가명처리
대상
데이터 항목</td><td colspan="2">• 학번, 과목, 학년, 성명, 성적(점수), 시도, 시군구, 읍면동, 지번, 거주지 유형, ㅇㅇㅇ, ㅁㅁㅁ, … (전체 20개의 컬럼)
• AA교육청 내 학생정보 100만명 중에서 B교육지원청과 C교육지원청에 속한 초등학교 및 중학교 학생에 대한 데이터</td></tr>
<tr><td rowspan="3">데이터
식별 위험성</td><td>식별성
유무</td><td>• 교육분야 개인정보 항목별 위험성 목록에 따라,
• 학번, 성명은 개인식별정보임 (중략)
• 위험성 목록에는 없는 ㅁㅁㅁ항목은 위험성 목록 CCC와 유사하므로 이를 준용하여 개인식별정보로 판단하고 위험성은 4로 판단</td></tr>
<tr><td>특이정보
유무</td><td>• 성적 점수의 특성상 최고점과 최하점은 특이정보로 인한 개인 식별성이 발생할 수 있음
• 주소와 거주지 유형(단독주택)에 따른 특이정보로 인한 개인 식별성이 발생할 수 있음</td></tr>
<tr><td>재식별시
영향도</td><td>• 민감한 거주지 유형과 성적 정보로 인한 재식별 발생 시 영향도가 일정 수준 있을 것으로 보임</td></tr>
<tr><td rowspan="3">처리 환경
식별 위험성</td><td>이용 및
제공 형태</td><td>• 교육청 내부 이용</td></tr>
<tr><td>처리 장소</td><td>• 교육청 내 별도 분석 공간을 마련하고 전용 분석 PC에서 사용
• 분석 공간에 대해 엄격한 출입통제 실시 및 관련 출입관리대장 기록·관리
• 분석PC는 인터넷 및 추가정보, 원본정보 및 다른 정보에 접근할 수 없도록 조치하여 분석할 예정임</td></tr>
<tr><td>다른 정보
결합 가능성</td><td>• 가명처리 전 개인정보를 교육청이 보관하고 있음</td></tr>
<tr><td>최종
검토의견*</td><td colspan="2">• 해당 연구는 교육청 내부에서 활용하는 것으로 데이터 자체 위험성과 처리환경 위험성을 고려할 때 다음과 같은 조치가 필요함
- 학번은 그 자체로 또는 결합시 식별될 가능성이 매우 높으므로 반드시 필요하지 않은 경우 삭제하고 그 과목별, 학년별 성적 추적을 위해 필요한 경우 학번을 그대로 사용하지 않도록 가명처리가 필요
- 성적은 결합 시 식별될 가능성이 있고 필요한 경우가 아니면 특정 항목은 삭제가 필요. 다만, 목적 달성에 필요한 경우에 한해 범주화하여 처리
※ 성적은 특이정보 가능성이 높으므로 범주화 등의 가명처리가 필요
- 지번의 경우 다른(공개된 정보 등) 정보를 통해 재식별 가능성이 있어 삭제 또는 목적 달성에 필요한 경우 가명처리 필요
• 그 외의 정보들은 재식별 가능성이 낮으며 목적 달성을 위해 필요하다고 판단되므로 가명처리 하지 않음</td></tr>
<tr><td colspan="3">[별첨] 식별 위험성 검토를 위한 근거 자료(검토서) 1부</td></tr>
</table>

가명정보 식별 위험성 검토 결과보고서(체크리스트 사용시)

<table>
<tr><td colspan="3">가명정보 활용목적</td><td>• AA교육청이 가명처리한 거주지별 학생정보와 성적 정보들을 A기관에 제공하여, 코로나로 원격학습에 따른 지역별 학업 성취도 격차를 파악하기 위한 연구 수행</td></tr>
<tr><td colspan="3">가명처리 대상 데이터 항목</td><td>• 학번, 과목, 학년, 성명, 성적(점수), 시도, 시군구, 읍면동, 거주지 유형, 지번, ㅇㅇㅇ,ㅁㅁㅁ, … (전체 20개의 컬럼)
• AA교육청 내 학생정보 100만명 중에서 B교육지원청과 C교육지원청에 속한 초등학교 및 중학교 학생에 대한 데이터</td></tr>
<tr><td colspan="3">이용기관의 개인정보보호수준</td><td>• 보호법 제28조의4(가명정보에 대한 안전조치 의무 등), ...등에 따른 법적 준수사항들을 모두 만족하고 있음</td></tr>
<tr><td rowspan="12">위험성검토</td><td rowspan="3">데이터</td><td>데이터 구성</td><td>• 총 6가지 항목에 대한 위험성 검토 결과 10 기준으로 3 수준으로 나타나 데이터 구성을 통한 식별 가능성은 낮은 편임</td></tr>
<tr><td>데이터 분포</td><td>• 총 2가지 항목에 대한 위험성 검토 결과 10 기준으로 3 수준으로 나타나 데이터 분포를 통한 식별 가능성은 낮은 편임</td></tr>
<tr><td>재식별 영향도</td><td>• 총 2가지 항목에 대한 위험성 검토 결과 10 기준으로 3 수준으로 나타나 재식별 영향도는 낮은 편임</td></tr>
<tr><td rowspan="4">처리환경</td><td>가명정보 처리 장소 및 형태</td><td>• 타 부서에서 자체 가명정보를 처리할 예정이며, 제한구역에서 처리하여 위험성은 10 기준으로 2 수준으로 매우 낮은 편임</td></tr>
<tr><td>다른정보 보유여부</td><td>• 총 5가지 항목에 대한 위험성 검토 결과 10 기준으로 2 수준으로 나타나 다른 정보와의 결합을 통한 식별 가능성은 매우 낮은 편임
※ 위탁 또는 제3자 제공하는 경우는 3가지 항목 해당(p.89 참고)</td></tr>
<tr><td>이용기관의 신뢰도</td><td>• 총 6가지 항목에 대한 위험성 검토 결과 10 기준으로 2 수준으로 나타나 이용기관의 신뢰도는 높은 편임</td></tr>
<tr><td>우연한 재식별</td><td>• 총 4가지 항목에 대한 위험성 검토 결과 10 기준으로 3 수준으로 나타나 우연한 재식별 가능성은 낮은 편임</td></tr>
<tr><td rowspan="5">경감</td><td>가명.익명처리*</td><td>• 해당사항 없음(수준 정의표에서 반영할 예정)</td></tr>
<tr><td>장소 통제 강화</td><td>• 안전구역(통제구역보다 강력한 통제 실시) 설정 및 해당 구역에서 가명정보 처리를 실시하여 총점에서 경감 -2점 실시</td></tr>
<tr><td>인원 통제 강화</td><td rowspan="3">• 해당사항 없음</td></tr>
<tr><td>인증 등 신뢰도</td></tr>
<tr><td>기타</td></tr>
<tr><td colspan="2">종합 검토 결과</td><td>• 식별 위험성에 대한 종합 검토 결과, 이용기관의 개인정보보호능력을 제외한 총 6가지 항목들에 대해 종합 위험성 점수는 80 기준으로 16 수준으로 나타나 전반적인 위험성은 약간 낮은 편임</td></tr>
<tr><td colspan="3">최종 검토 의견</td><td>• 해당 연구는 교육청 내부에서 활용하는 것으로 데이터 자체 위험성과 처리환경 위험성을 고려할 때 다음과 같은 조치가 필요함
- 학번은 그 자체로 또는 결합시 식별될 가능성이 매우 높으므로 반드시 필요하지 않은 경우 삭제하고 그 과목별, 학년별 성적 추적을 위해 필요한 경우 학번을 그대로 사용하지 않도록 가명처리가 필요
- 성적은 결합시 식별될 가능성이 있고 필요한 경우가 아니면 특정 항목은 삭제가 필요.(성적은 특이정보 가능성이 높아 가명처리 필요)
- 지번의 경우 다른(공개된 정보 등) 정보를 통해 재식별 가능성이 있어 삭제 또는 목적달성에 필요한 경우 가명처리 필요
- .....
• 그 외의 정보들은 재식별 가능성이 낮으며 목적 달성을 위해 필요하다고 판단되므로 가명처리 하지 않음</td></tr>
<tr><td colspan="4">[별첨] 식별 위험성 검토를 위한 근거 자료(체크리스트) 1부</td></tr>
</table>

4. 가명처리 방법 및 수준 정의표

가명처리 수준 정의표

순번	항목명	적용기술 및 처리수준	비고
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
…			

5. 기초자료 명세 : 데이터 특징

5.1 데이터 명세

가명정보 처리 기초자료명세서			
신청 기관 정보			
기관명			
주소			
데이터명		평가 목적	
데이터 수집			
이용 방법			
이용기간			
데이터 명세			
번호	구분	검토사항	
1	데이터 특징		
2	데이터 생성 방법		
3	데이터 제공방법		
4	데이터 관리 환경		

5.2 원본 데이터 세부 항목별 명세 예시

컬럼명	명세내용
등록번호	6자리수
환자명	XXX
입원일자	YYYYMMDD
퇴원일자	YYYYMMDD
입원과코드	영문 2자리(30 카테고리)
입원당시 주치의명	XXX
퇴원과코드	영문 2자리(30 카테고리)
퇴원당시주치의명	XXX
재원일수	3자리수
나이	3자리수
성별	F/M
진단코드	10자리 영문숫자혼합(첫자리 영문 대문자 나머지 숫자)
진단명	XXXXXXXXXX
우편번호	5자리수
주소	시(도)군구 도로명 번지
핸드폰번호	010-0000-0000
내원경위코드	1~5
암등록여부	0/1
퇴원형태	1~5
수술전재원일수	3자리수

5.3 원본데이터 예시

컬럼명	예시
등록번호	123456
환자명	홍길동
입원일자	20170321
퇴원일자	20170401
입원과코드	GS
입원당시 주치의명	XXX
퇴원과코드	MN
퇴원당시주치의명	강감찬
재원일수	12
나이	38
성별	F
진단코드	K330001123
진단명	Urinary Retention
우편번호	24312
주소	강원도 원주시 남원로 441
핸드폰번호	090-2222-3333
내원경위코드	3
암등록여부	0
퇴원형태	2
수술전재원일수	3

5.4 원본데이터 분포
(가능한 표 또는 그래프 형태와 참조 수치로 표현 권장)

항목	내용
■ 데이터 크기(레코드수/컬럼수)	950 GB (레코드 수: 500만건/ 컬럼 수: 12개)
■ 데이터 생성 방법	A사가 보유한 2020년 5월 부동산 시세정보에서 추출
■ 데이터 관리 환경 (기술적, 물리적)	접근통제, 계정관리, DB암호화 등이 적용된 DB서버에 저장

5.5 가명처리된 데이터의 세부 항목별 명세
(가명처리된 데이터로 5.2 형식을 참조하여 작성)

5.6 가명처리된 데이터 예시
(가명처리된 데이터로 5.3 형식을 참조하여 작성)

5.7 가명처리된 데이터 분포
(가명처리된 데이터로 5.4 형식에 맞게 가능한 표 또는 그래프 형태와 참조 수치로 표현 권장)

6. 가명정보 안전조치 이행 확약서

가명정보 안전조치 이행 확약서

본 기관은 「개인정보 보호법」에서 규정하고 있는 가명정보에 대한 안전조치의무등(제28조의4) 및 가명정보에 대한 안전성 확보 조치(시행령 제29조의5)를 성실히 이행하고 기타 관련 법령을 준수하였습니다.

아울러, 이를 이행•준수하지 아니하여 발생하는 관련 법적 책임을 부담할 것을 확약합니다.

년 월 일

신청기관 (직인)

※ 가명정보 안전조치 이행 확약서는 가명처리 기관과 가명정보 처리하는 기관이 동일할 경우(기관내 활용) 이행 확약서는 생략할 수 있음

적정성 검토 위원회 운영 세부 양식

1. 적정성 검토 결과서(위원용)

적정성 검토 결과서(위원용)

접수번호						
검토위원 정보	성명		소속		직위	

검토 대상	☐ 신규 ☐ 보완	
검토 일자	년 월 일 ~ 년 월 일	
최종검토결과	☐ 적정(승인) ☐ 조건부 승인 ☐ 부적정(반려)	
세부결과	가명정보 목적 적합성	☐ 적합 ☐ 미흡
	가명정보 이용항목 적합성	☐ 적합 ☐ 미흡
	식별 위험성 분석 보고서 적정성	☐ 적정 ☐ 미흡
	처리 수준 정의표 적정성	☐ 적정 ☐ 미흡
	처리 수준에 따른 처리 결과의 정확성	☐ 적정 ☐ 미흡
	처리 결과의 목적 달성 가능성	☐ 적정 ☐ 미흡
종합검토의견	※ 검토 결과가 조건부 승인인 경우 보완사항 및 부적정인 사유를 상세히 기재	

위와 같이 적정성 검토 결과를 통지합니다.

년 월 일

서명란	

2. 적정성 검토 종합결과서

적정성 검토 종합결과서

이용신청 접수번호	
검토 대상	☐ 신규 ☐ 보완
검토 일자	년 월 일 ~ 년 월 일
검토 결과	☐ 적정(승인) ☐ 조건부 승인 ☐ 부적정(반려)
종합 검토 의견	

위와 같이 적정성 검토 결과를 통지합니다.

년 월 일

서명란	위원장	검토위원	검토위원	사내 개인정보보호 책임자
	이름 (인)	이름 (인)	이름 (인)	이름 (인)

3. 비밀유지의무 서약서

비밀유지의무 서약서

본인은 가명처리 적정성 검토와 관련한 활동으로 얻어진 모든 정보에 대하여 XXXXXXX의 허락 없이 외부에 공개하지 않을 것을 서약합니다. 본 양식에 서명함으로써, 본인은 정보의 비밀을 지키기 위해 합당한 역할과 완전한 책임을 다 할 것에 동의합니다.

서 명 일: _____

소　　속: _____

성　　명: _____

서　　명: _____

○○○기관장　귀하

4. 이해상충 공개 서약서

이해상충 공개 서약서

접수번호	
가명정보 이용신청자명(기관명)	
적정성 검토 회의명	

본인은 상기 적정성 검토와 관련하여 가명정보 이용 신청자로부터 검토 결과에 영향을 미치는 지원과 제공에 대한 사항을 다음과 같이 확인하여 보고합니다.

순번	이해 관계 내용	예	아니오
1	적정성 검토 대상 가명정보를 이용할 예정이 있다.		
2	적정성 검토 대상 가명정보 활용에 대한 경제적•비경제적 이익을 가지고 있다.		
3	가명정보 이용신청자와 고용관계(상근, 비상근/공식, 비공식 등)에 있다.		
4	가명정보 이용신청자로부터 본 적정성 검토 비용 외에 검토 결과에 영향을 미칠 수 있는 경제적(1천만원 상당)•비경제적 이익을 제공받은 사실이 있다.		
5	본인 또는 배우자의 직계가족이 소속된 회사가 위에서 기술된 것과 같은 관계를 가지고 있다.		
6	그 밖에 적정성 검토 대상 가명정보 또는 가명정보 이용신청자와 이해관계가 있다.		

본인이 확인한 모든 내용은 정확히 기술되었으며 만약 평가 진행 중에 의뢰기관에 대한 이해관계가 변동되는 이해상충이 생기는 경우 이를 인지한 날로부터 5영업일 이내에 ○○○에 통지하겠습니다.

제출일: 년 월 일

서약자 : _____ (인)

[별지 13] 교육기관 분류체계별 개인정보 항목별 위험성 목록

교육분야 주요 개인정보 항목별 위험성 및 가명처리 방안 예시

※ 본 목록의 위험성은 참고사항으로 실제 가명처리시 결합 등 외부 환경적 요인에 따라 위험성이 증가할 수 있어 종합적인 위험성 검토가 전제되어야 함

대분류	중분류	항목명	위험성 크기	항목별 가명처리 방안
고유식별정보 등		주민등록번호	사용불가	사용불가
		여권번호	10	삭제
		운전면허번호	10	삭제
		외국인등록번호	10	삭제
		공공아이핀	9	삭제
		CI	9	삭제, 대체값 생성
		DI	9	삭제, 대체값 생성
개인식별정보		ID	8	삭제, 암호화
		사진	8	삭제
		이름	8	삭제, 암호화, 일련번호 대체
		휴대폰번호	8	삭제, 암호화, 일련번호 대체
		이메일주소	8	삭제, 암호화, 일련번호 대체
		아이행복카드번호	8	삭제, 암호화, 일련번호 대체
		계좌번호	8	삭제, 암호화, 일련번호 대체
		의료보험증번호	8	삭제, 암호화, 일련번호 대체
		의료보험가입정보	8	삭제, 암호화, 일련번호 대체
		차량번호	8	삭제, 암호화, 일련번호 대체
		참좋은카드번호	8	삭제, 암호화, 일련번호 대체
		체크카드번호	8	삭제, 암호화, 일련번호 대체
		복지카드번호	8	삭제, 암호화, 일련번호 대체
		신용카드번호	8	삭제, 암호화, 일련번호 대체
		교원번호	8	삭제, 암호화, 일련번호 대체
		교수번호	8	삭제, 암호화, 일련번호 대체
		연구자등록번호	8	삭제, 암호화, 일련번호 대체
		보훈번호	9	삭제, 암호화, 일련번호 대체
		장애인등록번호	9	삭제, 암호화, 일련번호 대체
		학번	7	삭제, 마스킹(*), 부분삭제, 그대로사용
개인식별가능정보		주소	6	시군구단위 범주화
		우편번호	6	앞3자리만, 그대로사용
		성별	6	삭제, 마스킹(*), 코드화, 그대로사용
		진학학교	4	삭제, 마스킹(*), 범주화(초등학교, 중학교 등 단위), 그대로사용
		의료보험종류	2	삭제, 범주화(지역가입, 직장가입 등 단위), 그대로사용

대분류	중분류	항목명	위험성 크기	항목별 가명처리 방안
		직업	4	삭제, 범주화(9등급->3등급 등), 그대로 사용
		직위	2	삭제, 범주화, 그대로사용
		직책	2	삭제, 범주화, 그대로사용
		직급	2	삭제, 범주화, 그대로사용
		본적지 주소	6	시군구단위 범주화
		출생지	6	시군구단위 범주화
		국적	6	삭제, 본국 인구 10만명미만 삭제, 그대로사용
		비자번호	6	삭제, 부분삭제, 그대로사용
		학교명	4	삭제, 마스킹(*), 범주화(초등학교, 중학교 등 단위), 그대로사용
		학급명	4	삭제, 마스킹(*), 범주화, 그대로사용
		고등학교 코드	4	삭제, 마스킹(*), 범주화(상위 레벨로), 그대로사용
		고등학교명	4	삭제, 마스킹(*), 범주화(초등학교, 중학교 등 단위), 그대로사용
		성적	4	삭제, 마스킹(*), 범위(구간으로), 그대로사용
		교과목별 성적	4	삭제, 마스킹(*), 범위(구간으로), 그대로사용
		모의고사 성적	4	삭제, 마스킹(*), 범위(구간으로), 그대로사용
		전공	2	삭제, 마스킹(*), 일반화(상위레벨로), 그대로사용
		학년	2	삭제, 마스킹(*), 범위(구간으로), 그대로사용
		반	2	삭제, 마스킹(*), 범위(구간으로), 그대로사용
		번호	2	삭제, 마스킹(*), 범위(구간으로), 그대로사용
		학업성취도	4	삭제, 마스킹(*), 범위(구간으로), 그대로사용
		국가학업성취도	4	삭제, 마스킹(*), 범위(구간으로), 그대로사용
		성취도	4	삭제, 마스킹(*), 범위(구간으로), 그대로사용
		특수 교육관련 서비스	5	삭제, 마스킹(*), 일반화(상위 레벨로), 그대로사용
		전입&전출사항	2	삭제, 마스킹(*), 그대로사용
		식습관, 수면습관 등 유아생활 기초정보	4	삭제, 마스킹(*), 그대로 사용

대분류	중분류	항목명	위험성 크기	항목별 가명처리 방안
		우유종류	1	삭제, 마스킹(*), 일반화(상위 레벨로), 그대로사용
		가족관계	4	삭제, 마스킹(*), 그대로 사용
		결석사유	2	삭제, 그대로 사용
		결석일수	4	삭제, 그대로 사용
		출결현황	2	삭제, 그대로 사용
		사업자등록번호	8	삭제, 부분삭제, 마스킹(일부), 그대로사용
		담임성명	7	삭제, 마스킹(김OO, 홍OO), 그대로사용
		대출도서목록	2	삭제, 그대로 사용
		자격증 및 인증취득 현황	2	삭제, 그대로 사용
		가입 인터넷 통신사	2	삭제, 그대로 사용
		봉사 및 체험활동 상황	2	삭제, 그대로 사용
		교과학습발달상황	4	삭제, 그대로 사용
		창의적 체험활동 상황	2	삭제, 그대로 사용
		기탁자관리	7	삭제, 마스킹(*), 일반화(상위 레벨로), 그대로사용
		기부자 인적사항	10	삭제, 마스킹, 일반화(상위 레벨로), 그대로사용
		수상 여부	3	삭제, 마스킹, 가/부 또는 0/1로 표기, 그대로사용
		수상 및 경력사항	5	삭제, 마스킹, 일반화(상위 레벨로), 그대로사용
		상벌기록	4	삭제, 마스킹, 일반화(상위 레벨로), 그대로사용
		IP주소	8	삭제, 부분삭제, 마스킹, 그대로사용(고유주소의 경우 삭제)
		이수과정	2	삭제, 그대로 사용
		이수시간	1	삭제, 그대로 사용
		희망진로	2	삭제, 일반화(상위 레벨로), 그대로사용
		흥미 및 특기	2	삭제, 그대로 사용
		성적증명서	8	삭제, 개인정보 마스킹
		성적통지표	8	삭제, 개인정보 마스킹
		재직 사업체 매출액	4	삭제, 라운딩, 상하단코딩
		연구책임자	8	삭제, 마스킹(김OO, 홍OO), 그대로사용
		참여과제번호	8	삭제, 부분삭제, 마스킹(일부), 그대로사용
		교단 및 교파	6	삭제, 일반화(상위 레벨로), 그대로사용
		교직유무	2	삭제, 그대로 사용

대분류	중분류	항목명	위험성 크기	항목별 가명처리 방안
		연수성적	4	삭제, 범위(구간으로), 그대로사용
		출산자녀수	6	삭제, 그대로 사용
		학위정보	2	삭제, 일반화(상위 레벨로), 그대로사용
		건물소유 여부	1	삭제, 그대로 사용
		건물소유 형태	1	삭제, 일반화(상위 레벨로), 그대로사용
		고용 형태	2	삭제, 일반화(상위 레벨로), 그대로사용
		보수월액	4	삭제, 라운딩, 상하단코딩
		쌍생아 여부	6	삭제, 그대로 사용
개인식별가능정보	민감정보(날짜)	생년월일	6	삭제, 연까지만, 연월까지만, 연월일에서 일자 노이즈처리
		입학일	4	삭제, 노이즈처리, 그대로 사용
		입학년도	4	삭제, 그대로 사용
		수료일	4	삭제, 노이즈처리, 그대로 사용
		졸업일	4	삭제, 노이즈처리, 그대로 사용
		졸업년도	4	삭제, 그대로 사용
		가입일	5	삭제, 노이즈처리, 그대로 사용
		임기일	5	삭제, 노이즈처리, 그대로 사용
		변동년도	5	삭제, 그대로 사용
		자격증 발급일자	4	삭제, 노이즈처리, 그대로 사용
		입원일자	6	삭제, 연까지만, 연월까지만, 연월일에서 일자 노이즈처리
		퇴원일자	6	삭제, 연까지만, 연월까지만, 연월일에서 일자 노이즈처리
		재해일자	6	삭제, 연까지만, 연월까지만, 연월일에서 일자 노이즈처리
		진료일자	6	삭제, 연까지만, 연월까지만, 연월일에서 일자 노이즈처리
		진료기간	6	삭제, 그대로 사용
		마약투약일자	6	삭제, 연까지만, 연월까지만, 연월일에서 일자 노이즈처리
		개장예정 연월일	4	삭제, 연까지만, 연월까지만, 연월일에서 일자 노이즈처리
		개설예정일	4	삭제, 연까지만, 연월까지만, 연월일에서 일자 노이즈처리
		개원예정일	4	삭제, 연까지만, 연월까지만, 연월일에서 일자 노이즈처리
		고발조치일	4	삭제, 연까지만, 연월까지만, 연월일에서 일자 노이즈처리
		교지년월	2	삭제, 그대로 사용

대분류	중분류	항목명	위험성 크기	항목별 가명처리 방안
	민감정보 (건강)	키	4	삭제, 범위(구간으로), 그대로사용
		몸무게	4	삭제, 범위(구간으로), 그대로사용
		혈액형	4	삭제, 그대로 사용
		시력검사결과	2	삭제, 그대로 사용
		청력검사결과	2	삭제, 그대로 사용
		진찰소견	3	삭제, 개인정보 마스킹, 개인정보 없는 경우 그대로사용
		간염검사결과	2	삭제, 그대로 사용
		구강검사결과	2	삭제, 그대로 사용
		병리검사결과	2	삭제, 그대로 사용
		X-Ray	4	삭제, 개인정보(DICOM 메타파일 내) 삭제
		DNA	9	삭제원칙, 예외적으로 허용 (보건의료데이터활용가이드라인 참조)
		지문	9	삭제원칙, 예외적으로 허용 (보건의료데이터활용가이드라인 참조)
		홍채	9	삭제원칙, 예외적으로 허용 (보건의료데이터활용가이드라인 참조)
		체지방률	2	삭제, 그대로 사용
		비만도	2	삭제, 그대로 사용
		신체의 능력	2	삭제, 그대로 사용
		전염병 예방접종	2	삭제, 그대로 사용
		결핵검사	2	삭제, 그대로 사용
		소변검사	2	삭제, 그대로 사용
		출생시 체중	2	삭제, 그대로 사용
		예방접종현황	2	삭제, 그대로 사용
		신체발달사항	2	삭제, 그대로 사용
		신체의 능력	2	삭제, 그대로 사용
		검진결과	2	삭제, 그대로 사용
		건강검진결과	2	삭제, 그대로 사용
		건강검진현황	2	삭제, 그대로 사용
		건강상태 및 발달적 정보	2	삭제, 그대로 사용
		별도 검사 현황	4	삭제, 마스킹, 그대로사용
		가족력	2	삭제, 일반화(상위 레벨로), 그대로사용
		과거 질병(병력)	4	삭제, 일반화(상위 레벨로), 그대로사용
		복용중인 약물	4	삭제, 일반화(상위 레벨로), 그대로사용

대분류	중분류	항목명	위험성 크기	항목별 가명처리 방안
		보유질환	4	삭제, 일반화(상위 레벨로), 그대로사용
		알레르기	2	삭제, 그대로 사용
		진단명	4	삭제, 그대로 사용
		감염상태	4	삭제, 그대로 사용
		접종상태	2	삭제, 그대로 사용
		진료기록	8	세부 항목별로 보건의료 데이터활용가이드라인 참조
		투약기록	8	세부 항목별로 보건의료 데이터활용가이드라인 참조
		검사항목 및 검사결과	2	세부 항목별로 보건의료 데이터활용가이드라인 참조
	민감정보 (일반)	기초생활수급자 여부	6	삭제, 마스킹(*), 그대로 사용
		기초생활수급자 증명서	6	삭제, 개인정보 마스킹, 개인정보 없는 경우 그대로사용
		차상위계층증명서	6	삭제, 개인정보 마스킹, 개인정보 없는 경우 그대로사용
		다문화가정 여부	6	삭제, 마스킹(*), 그대로 사용
		복지대상자 여부	4	삭제, 마스킹(*), 그대로 사용
		복지카드 급수	6	삭제, 범주화(9등급->3등급 등), 그대로 사용
		국가보훈대상	4	삭제, 마스킹(*), 그대로 사용
		발달평가 결과	2	삭제, 마스킹, 범주화, 그대로사용
		장애구분	6	삭제, 마스킹(*), 그대로 사용
		장애등록 여부	6	삭제, 마스킹(*), 그대로 사용
		장애진단명	6	삭제, 일반화(상위 레벨로), 그대로사용
		장애유형	6	삭제, 일반화(상위 레벨로), 그대로사용
		장애정도	6	삭제, 일반화(상위 레벨로), 그대로사용
		장애등급	6	삭제, 범주화(9등급->3등급 등), 그대로 사용
		장애진단검사결과	6	삭제, 마스킹, 범주화 또는 일반화, 그대로사용
		지능지수	2	삭제, 범위(구간으로), 그대로사용
		범죄경력자료	6	삭제, 개인정보 마스킹, 개인정보 없는 경우 그대로사용
		마약처방종류	6	삭제, 그대로 사용(마약관련 데이터만 있는 경우)
		마약 투약량	6	삭제, 마약관련 데이터만 있는 경우(범위, 그대로사용)

대분류	중분류	항목명	위험성 크기	항목별 가명처리 방안
		사상 • 신념	4	삭제, 일반화(상위 레벨로), 그대로사용
		노동조합 • 정당의 가입 • 탈퇴	4	삭제, 일반화(상위 레벨로), 그대로사용
		정치적 견해	4	삭제, 범주화 또는 일반화, 그대로사용
		건강	8	세부 항목별로 보건의료 데이터활용가이드라인 참조
		성생활	3	삭제, 마스킹, 범주화 또는 일반화, 그대로 사용
		유전정보	8	삭제원칙, 예외적으로 허용 (보건의료데이터활용가이드라인 참조)
		개인별 대출이력	6	삭제, (은행명(마스킹), 건수(범위화), 금액(라운딩)), 그대로사용