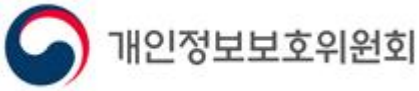
교육분야 가명·익명정보 처리 가이드라인

2020. 11.



가이드라인 활용 안내

□ **개 요**

본 가이드라인은 교육분야 개인정보를 가명정보 및 익명정보로 처리하는 절차와 방법에 대한 내용을 제공하는 자료로써 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 2020년 11월 기준으로 작성되었습니다. 항상 최신의 가이드라인은 교육부 개인정보보호 포털(자료실→참고자료)에서 확인하시기 바랍니다.

목 차

제 Ⅰ 편

가이드라인 개요

1. 배경 및 목적
2. 적용 범위
3. 용어 정리

1 배경 및 목적

○ 개정된 「개인정보 보호법」('20.8.5.시행)에서는 가명정보 처리에 관한 특례가 신설되어 개인정보처리자가 통계작성, 과학적 연구, 공익적 기록보존 등을 위해 개인정보를 가명처리하여 활용할 수 있는 기반 마련

○ 4차 산업혁명 시대를 맞아 핵심 자원인 데이터의 이용 활성화를 통한 신산업 육성이 범국가적 과제로 대두되고 있고 교육정보 활용을 위한 가명정보의 처리 및 결합 등에 대한 수요 증가가 예상됨에 따라 교육분야 특수성을 고려한 가명정보 처리 체계 마련 필요

○ 이에 본 가이드라인은 교육분야의 가명·익명정보를 처리하는 과정에서 발생할 수 있는 개인정보 오·남용을 방지하고 안전한 가명정보 처리 방안을 제시하여 보다 풍부하고 다양한 교육정보 활용을 통한 효율적 교육정책 수립 등을 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, '20.9.)

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 개인정보 처리자와 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

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 특정개인을 알아볼 수 없는 정보

※ 개인정보에 대한 판단은 개인정보처리자가 보유한 정보 또는 접근 가능한 권한 등 상황에 따라 상이

○ 개인식별정보(식별자)

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

○ 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 일부를 드러낼 수 있는 정보

※ 개인식별가능정보는 다른 속성과 결합할 경우 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 가능

○ 가명처리

- 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가정보가 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 데 이용된 수단이나 방식(알고리즘, Salt 값 등), 가명정보와의 비교·대조 등을 통해 삭제 또는 대체된 개인정보 부분을 복원할 수 있는 정보(매핑 테이블 정보, 가명처리에 사용된 개인정보 등)

※ 추가정보(원본정보와 알고리즘·매핑테이블 정보 등)와 가명정보는 시행령 제30조 또는 제48조의2에 따른 안전성 확보조치 및 각각 정보의 분리보관, 접근 권한의 분리를 하여야 함

○ 특이정보

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

○ 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

○ 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

※ 가명정보를 추가정보 또는 처리자가 보유하고 있는 개인정보나 공개된 정보와의 결합 또는 대조·비교 등을 통해 정보주체가 누구인지 확인할 수 있는 상태로 회복시키기 위한 처리 일체

○ 개인정보파일

- 정보를 체계적으로 관리하거나 처리할 목적으로 일정한 규칙에 따라 구성되거나 배열된 둘 이상의 정보들

○ 결합키

- 결합 대상 가명정보의 일부로서 해당 정보만으로는 특정 개인을 알아볼 수 없으나 다른 정보주체와 구별할 수 있도록 조치한 정보

※ 내부 결합 시에는 결합키로, 전문기관을 통한 결합의 경우에는 결합키 연계정보 생성을 위한 정보로 사용됨

○ 결합키연계정보

- 동일 정보주체에 대해 가명정보를 결합할 수 있도록 서로 다른 결합신청자 간의 결합키를 연계한 정보

○ 결합신청자

- 가명정보의 결합을 신청하는 개인정보처리자 또는 기관

※ 가명정보를 제공만 하는 자, 가명정보를 제공하고 결합한 정보를 이용하는 자 또는 가명정보의 제공 없이 결합한 정보를 이용하는 자를 모두 포함

○ 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 보호위원회가 지정하여 고시하는 기관

○ 반출처리공간

- 결합신청자가 결합된 정보를 반출하기 전 추가 가명·익명처리를 위해 기술적·관리적·물리적으로 안전성 확보 조치한 공간

○ 다른정보

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

※ 가명정보처리자, 가명정보취급자가 보유하고 있거나 합리적으로 입수 가능한 정보에 한함

제 II 편

가명처리

1 개 요

❖ 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 취업지 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, 학생보건 분야에서 공익을 위해 시행되는 연구 등을 포함

▸ (예시) 교육부가 학생의 학습 및 미래 보장을 위해 학생생활기록부, 건강기록부, 출결 정보 등을 심층 분석하여 위기징후* 탐지 알고리즘을 연구하여 새로운 서비스(시스템)을 구축·운영하려는 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 인물정보를 기록하여 보관하는 경우

□ 가명처리 원칙

○ 가명처리 대상은 법률에서 허용한 목적 내에서 개인정보를 정보주체의 추가적인 동의 없이 수집 목적 외로 이용 가능

• 고유식별정보는 직접 식별자에 해당하므로 고유식별정보가 남아 있거나 역추적이 가능하도록 해서는 안 됨

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

○ 개인정보를 가명처리하여 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 취급권한 분리

– 가명처리를 수행하는 자와 가명정보의 적정성을 검토하는 자*, 가명정보취급자(활용 등)는 관리적·기술적으로 권한을 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 보완 통제 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

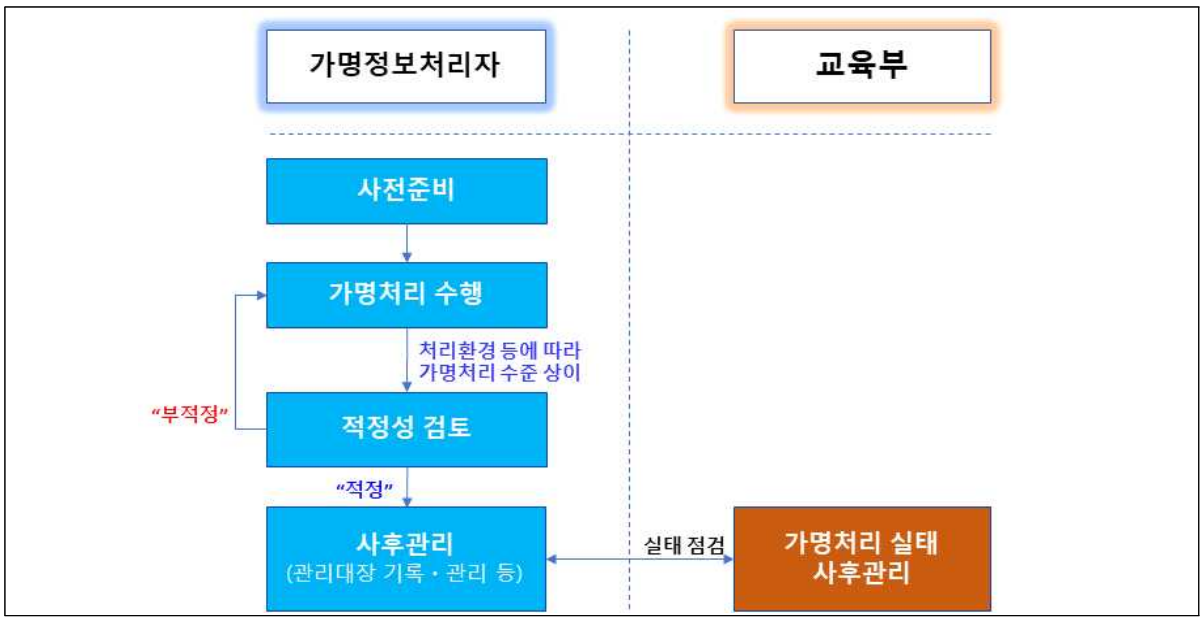
– 가명정보를 제공받는 자는 해당 가명정보의 가명처리 참여 불가

❍ 안전한 가명처리 방법을 적용하여 가명정보를 변환하도록 함

❍ 개인정보처리자는 가명정보 처리업무를 외부에 위탁하는 경우, 위탁계약서 등에 안전성 확보조치 관련 내용들을 포함하여 진행

❍ 개인정보처리자는 가명처리를 수행하는 자 등에 대해 년 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 개인정보를 선정

○ **(가명처리)** 가명처리 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 가능성 검토

※ "부적정" 판단 시 추가 가명처리를 위해 가명처리 단계로 이동

○ **(사후관리)** 가명처리된 가명정보와 추가정보에 대해 안전성 확보조치를 수행하고, 재식별 모니터링 및 재식별사고 발생에 관한 대책 수립 및 이행

○ **(가명처리 실태 사후관리)** 가명처리 현황 및 안전성 확보 조치 등에 대해 조사·점검 등을 실시

□ 가명처리 예시

[개인정보와 속성자 특징]

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 속성자 특징 예시

· 성별/혈액형별 나이와 전공 및 학위에 대한 상관관계 연구 목적으로 가명정보를 만들 경우 '성명', '연락처'는 직접적으로 개인이 식별 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 기법 중 하나인 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 가명 조치 없이 그대로 활용

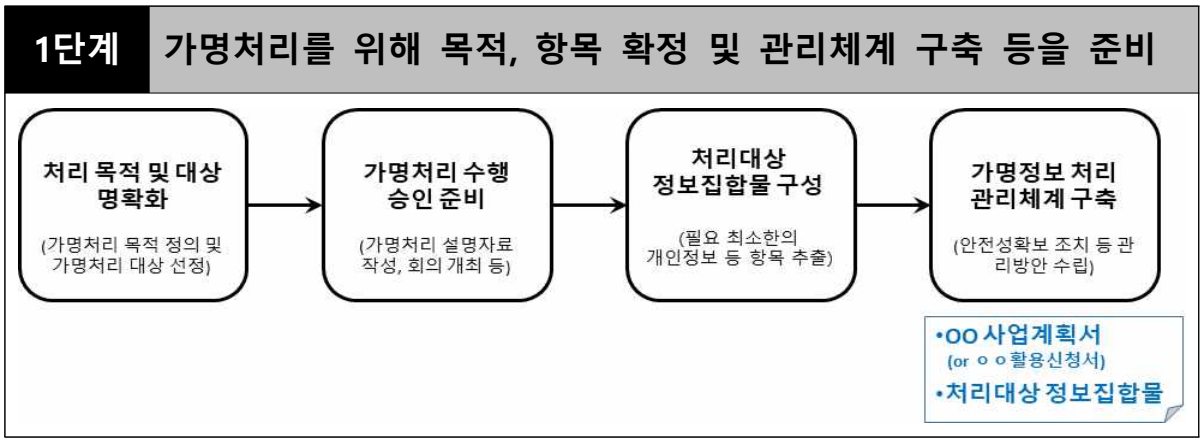
성명	연락처	성별	생년월일	혈액형		전공	학위
				ABO	RH		
		여	1965~~0512~~	A	Rh+	법학	박사
		남	1967~~1212~~	B	Rh+	컴퓨터	학사
		여	1968~~1015~~	O	Rh+	건축	학사
		~~남~~	~~19920721~~	~~AB~~	~~Rh-~~	~~보안~~	~~학사~~
		남	1993~~0423~~	AB	Rh+	교육	학사
		남	1994~~0925~~	O	Rh+	음악	학사
		〃	〃	〃	〃	〃	〃

[표 2] 개인정보 가명처리 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, 연구(산업적 연구 포함), 공익적 기록보존 목적 등

○ **(가명처리 수행 승인)** 가명처리 관련 계획수립 및 회의 개최 등을 통해 기관장 또는 개인정보 보호책임자* 승인 후 가명처리 수행

* 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자(법 31조, 시행령 제32조, 지침 21조)

☞ 주요 처리 사항

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

※ 제Ⅱ편 > 3. 가명정보의 안전한 관리 > 관리적 보호조치, 가명정보 제3자 제공 관련 계약서 포함 사항 참조

※ 타 기관과 가명정보를 결합 제공하는 경우도 동일

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

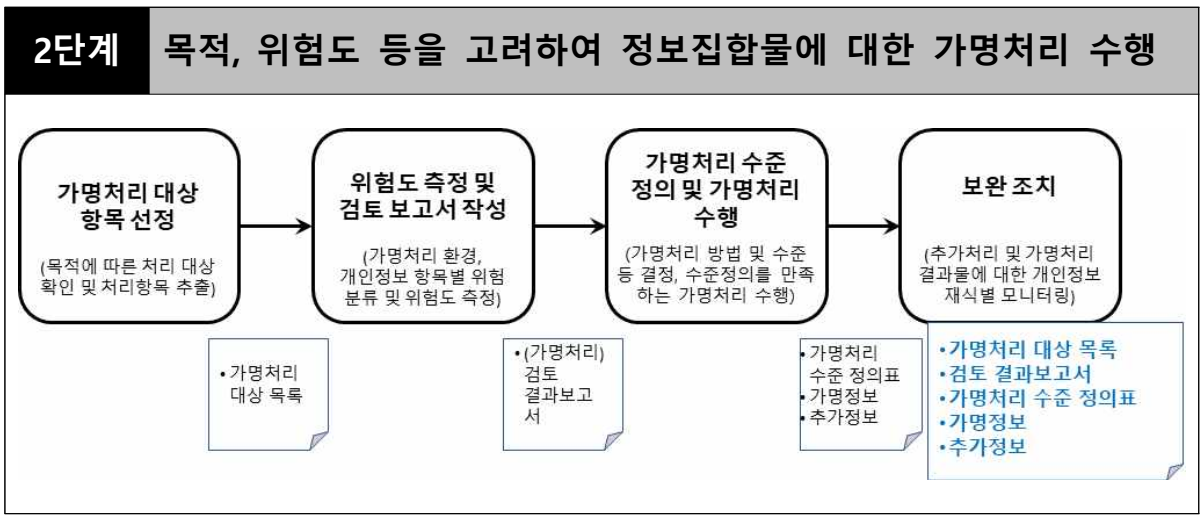
○ **(가명정보 처리 관리체계 구축)** 가명정보를 안전하게 보호할 수 있는 관리방안을 수립하고 추가정보 등에 대한 접근관리 체계 구축

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

주요 산출물

- 사업계획서
- 처리대상 정보집합물(개인정보)

2-2 가명처리 수행 (2단계)



<그림 3> 가명처리 수행 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

※ 분석 목적과 상관없는 개인정보 및 기타 정보는 대상 선정에서 제외

□ 위험도 측정 및 검토보고서 작성

○ **(처리환경별 위험도 측정)** 가명처리 환경과 개인정보 항목별 위험도를 분류하고 이를 기반으로 개인정보 위험도 측정

1. 가명처리 환경에 따른 위험도 분류

– 처리 목적에 따라 처리(제공)환경과 제공받는 자의 개인정보 보호수준 및 다른 정보 보유여부 등을 검토

※ 불특정 제3자(공개 등)에게 제공하는 경우 익명정보로 처리하는 것을 원칙

처리환경				기관의 개인정보 보호수준*	재식별수준 (다른정보 보유 등)**
활용장소	활용처	처리유형	기관유형		
내부	소유부서	활용	교육기관	상	상
외부	타부서	제공	민간기관	중	중
		결합		하	하

[표 3] 처리환경별 위험도 분류 고려사항 예시

* 처리자나 또는 제공받는 자의 안전조치 수준 : 내부통제 위험도 등 안전성 확보조치에 관한 사항 '가명정보의 안전한 관리를 위한 법제적 요구사항'(별지 9) 참조

** 개인정보처리자가 보유한 다른 정보나 혹은 제공받는 자가 보유한 다른 정보와의 연결을 통해 특정 개인을 알아볼 가능성

– 처리(제공)환경과 정보집합물의 규모, 정보의 정확성 수준 등을 고려하여 다양한 요소를 가감할 수 있음

※ 예시) 활용처를 소유부서, 특정 타부서, 전체부서 등으로 추가, 개인정보 보호수준 및 재식별 수준 상-중-하, 1급~5급 등 단계 다양화 등

[처리환경별 위험도 분류 예시]

· ㅇㅇ교육청이 A부서의 A1 개인정보를 가명처리하여 B부서에서 사용하며 보호수준은 높고, 재식별 가능성은 낮은 상태라고 가정할 경우

처리환경				기관의 개인정보 보호수준**	재식별수준 (다른정보 보유 등)**
활용장소	활용부서	처리유형	기관유형		
내부(1)	소유부서(1)	활용(1)	**교육기관(1)**	**상(1)**	상(3)
외부(2)	**타부서(2)**	**제공(2)**	민간기관(2)	중(2)	중(2)
		결합(3)		하(3)	**하(1)**

[표 4] 처리환경별 위험도 분류 측정 예시

※ 예시 표에서 점수는 처리환경의 다양성을 고려하여 가명정보처리자가 판단하여 점수 배정

· 각각의 분류 기준의 점수를 합산하여 처리환경 1+2+2+1=6점, 보호수준 1점, 재식별수준 1점, 총 8점으로 산정하고 점수가 높을수록 위험도가 높은 처리환경으로 판정할 수 있음

· 처리환경별 위험도 점수별 가명처리 방안을 마련하여 해당 방안을 적용

2. 개인정보 항목별 위험도 분류

– 기관 자체적으로 개인정보 분류체계를 작성하고 해당 분류체계에 따른 위험도를 분류하여 적용

[항목별 위험도 분류 예시]

분류	항목	위험도
고유식별정보	주민등록번호	사용불가
	여권번호, 운전면허번호, 외국인등록번호	10
개인식별정보	상세주소	6
〃	〃	〃

○ **(가명처리 검토 결과보고서 작성)** 가명정보처리자는 가명처리 환경 위험도와 항목별 위험도를 종합적으로 고려하여 가명처리에 대한 위험도 평가 결과 도출

- 가명정보 활용에 따른 처리 환경과 개인정보 분류를 통해 도출된 위험도를 기반으로 '가명처리 검토 결과보고서'(별지 1) 작성 관리

□ 가명처리 수준 정의 및 가명처리 수행

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

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

- 가명처리 단계에서 생성되는 추가정보는 삭제하는 것을 원칙으로 하되, 시계열분석 등과 같이 불가피하게 저장하여야 하는 경우 분리 보관

※ 세부사항은 Ⅱ편 > 3. 가명정보의 안전한 관리 > 기술적 보호조치 참고

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

□ 보완조치

○ **(특이정보 처리)** 가명처리된 정보에서 개인이 식별될 가능성이 높은 특이정보를 확인하여 추가적으로 가명처리

▸ 수능 만점자, 국내 최고령, 최장신, 고액 체납금액, 고액 장학금기부자 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』> '참고자료 2. 특이정보 정의 및 처리사례'를 참조하여 처리

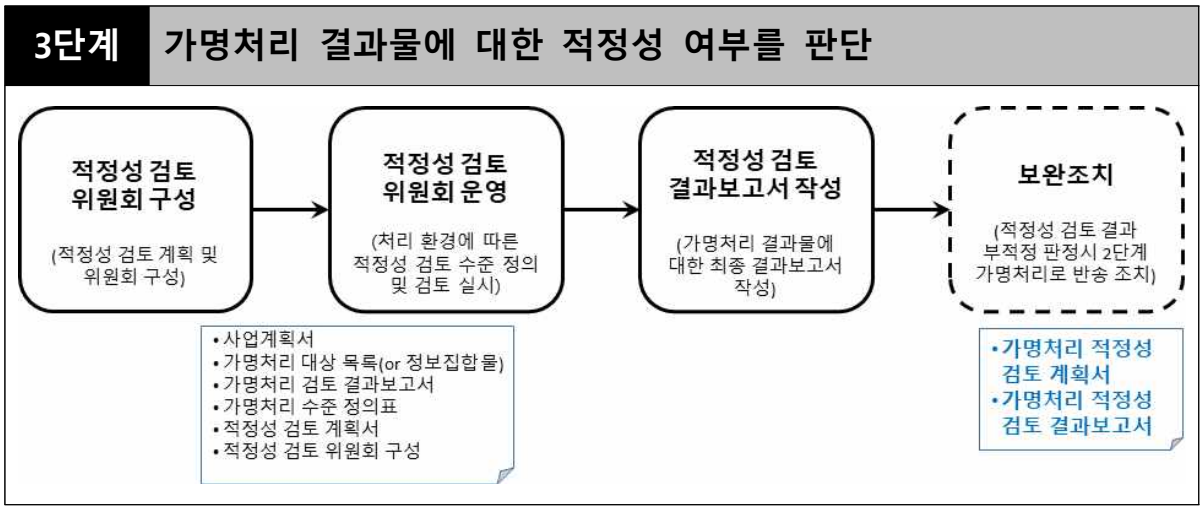
– 특이정보를 처리하는 과정에서 변경사항 발생 시 필요한 경우 기존에 작성된 '가명처리 검토 결과보고서'(별지 1)나 '가명처리 수준 정의표'(별지 2)에 해당 내용 반영

○ **(목적 달성을 위한 추가 가명처리)** 목적 달성이 어려운 경우 목적 달성에 필요한 수준을 고려하여 추가 가명처리 수행

주요 산출물

- 가명처리 대상 목록
- 가명처리 검토 결과보고서
- 가명처리 수준 정의표
- 가명정보, 추가정보

2-3 적정성 검토 (3단계)



<그림 4> 가명처리 적정성 검토 단계 세부 절차

□ 적정성 검토 위원회 구성

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

* 내부적으로 가명처리 적정성을 검토하되 필요시 별도 위원회 구성 가능

– **(위원 자격 및 인원)** 개인정보보호, 가명처리 기법 등에 관한 학식과 경험이 풍부한 사람으로 다음 각 호에 해당하는 사람을 고루 포함하여 3명 이상 7명 이내의 위원으로 구성

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 보호와 관련한 경력과 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)** 가명정보 처리의 적정성 및 가명정보를 제3자에게 제공하는 경우 제공의 적정성 등 검토

- **(위원장)** 위원 중 호선으로 정하거나 위원으로 임명된 가명정보 처리기관의 개인정보보호책임자 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 참고

□ 적정성 검토 위원회 운영

○ 위원회는 적정성 검토 필요 발생 시 구성 운영토록 하며, 개인정보처리자는 사전에 이에 대한 인력풀을 구성 운영할 수 있음

※ 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

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

○ 가명정보처리자는 적정성 검토를 위한 기초자료*를 준비

* 사업계획서, 가명처리 검토 결과보고서, 가명처리 수준 정의표 등

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	가명처리 검토 결과보고서, 가명처리 수준 정의표
가명처리 수준 기준	가명처리 수준 정의표
기타 프라이버시 보호모델 적용 여부 등이 기초자료에 포함이 가능	가명처리 수준 정의표 또는 가명처리 검토 결과보고서

[표 5] 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 가명정보의 재식별 의도 및 능력과 가명정보 보호수준, 신뢰도 등을 고려하여 가명정보의 제공이 적정한 지 종합적으로 검토

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

□ 적정성 검토 결과보고서 작성

○ 위원회는 적정성 검토 결과에 대해 '가명처리 검토 결과보고서'(별지 1) 및 '가명처리 수준 정의표'(별지 2)를 참고하여 '적정성 검토 결과보고서'(기관별 자유 양식) 작성

□ 보완조치

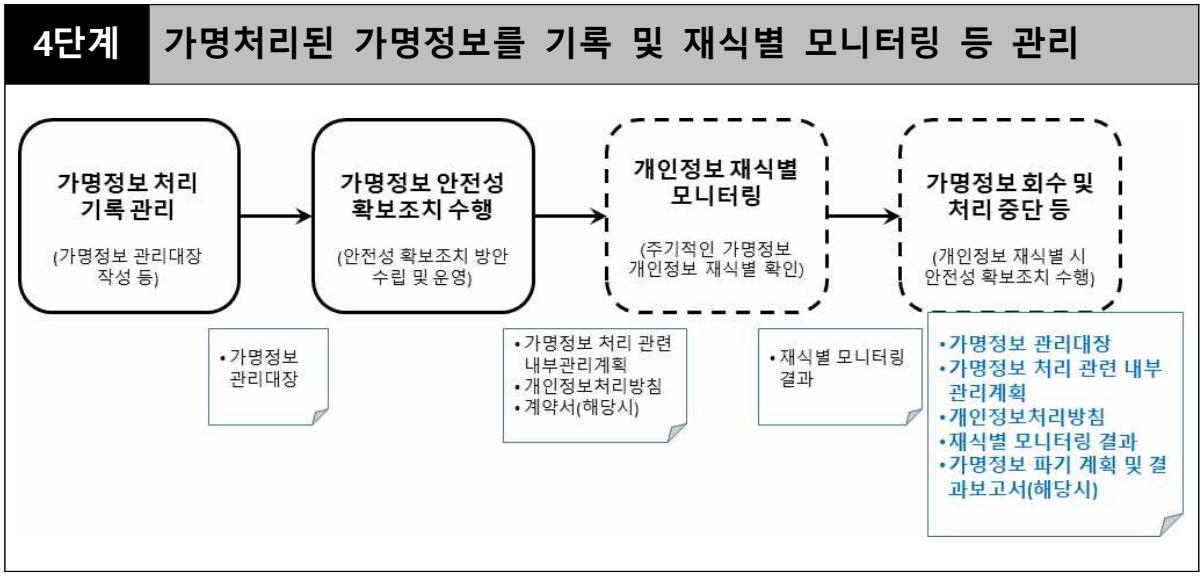
○ 적정성 검토 결과 "부적정" 판정 시 가명정보의 활용·제공 계획을 중단하거나, 가명정보 활용을 계속하고자 한다면 2단계인 "가명처리" 단계로 돌아가 추가적인 가명처리 조치를 해야 함

※ 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)
- 가명처리 적정성 검토 결과보고서(검토 시 추가처리 한 경우 해당 내용 포함)

2-4 사후관리 (4단계)



<그림 5> 가명처리 사후관리 단계 세부 절차

○ **(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 제공시 제공받는 자, 처리 및 보유기간, 추가정보의 이용 및 파기 등

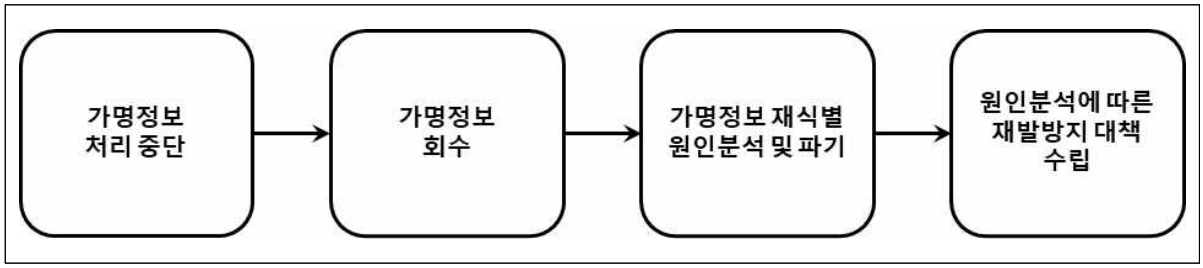
○ **(안전성 확보조치 수행)** 가명정보처리자(제공·활용하는 자)는 가명정보의 안전한 관리를 위한 내부관리계획의 수립 등 법령에서 요구하는 관련 조치 수행

– 가명정보 처리 관련 주요 사항을 내부관리계획에 포함하여 수립하고 개인정보처리방침에 공개

○ **(재식별 모니터링)** 가명정보처리자(활용자)는 가명정보 보유기간 동안 개인정보 재식별 가능성이 증가하는 지 여부 등을 지속적으로 모니터링하고 정기적으로 점검(년 1회 이상 권고)

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

* 필요 시 개인정보처리자는 내부관리계획 또는 별도의 가명정보 처리 지침(기관 자체 수립) 등에 재발방지 방안 수립 가능



<그림 6> 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 내부관리계획 (기존에 존재할 경우 불필요)
- 개인정보처리방침 : 홈페이지에 해당 내용 공개
- 재식별 모니터링 점검 결과(연 1회 이상)

※ 가명정보를 제3자에게 제공하는 경우 적정성 검토(3단계) 완료 이후 계약서를 작성하고 사후관리(4단계)에서는 작성한 '계약서'를 산출물로 관리(해당 시)

3 가명정보의 안전한 관리

□ 관리적 보호조치

○ **(가명정보 처리 내부관리계획 수립·시행)** 가명정보 처리 관련 내용을 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
라. 가명정보 처리 기록 작성 및 보관에 관한 사항
마. 개인정보 처리방침 공개에 관한 사항
바. 가명정보의 재식별 금지 등 오남용 제한에 관한 사항
사. 가명정보 재식별 발생 시 대응조치

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

○ **(개인정보처리방침 공개)** 가명정보 처리내용을 포함·공개

☞ 개인정보처리방침에 포함 사항

가. 가명정보의 처리 목적
나. 가명정보의 처리 및 보유 기간(필요시)
다. 가명정보의 제3자 제공에 관한 사항 (해당시)
라. 가명정보 처리의 위탁에 관한 사항 (해당시)
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 계약서*에 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 (금지는 아님)
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 기록 관리하고 년 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 접근통제가 적용되어야 함

○ **(접근 권한 관리)** 개인정보처리자는 가명정보 또는 추가정보에 접근할 수 있는 담당자를 가명정보 처리 업무 목적 달성에 필요한 최소한의 인원으로 지정하고 접근권한은 업무에 따라 차등부여 하여야 함

※ 시행령 제29조의5(가명정보에 대한 안전성 확보 조치) 제1항 제3호 "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

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

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 처리시 해당 검색조건문(쿼리)을 정보주체 정보로 기록이 가능 • 가명정보의 특성상 추가정보의 사용 없이는 정보주체 식별이 불가능하므로 본 항목에는 실제 정보주체의 정보가 아니라 어떠한 가명정보를 처리했는지를 추적할 수 있는 정보를 기록할 수 있음
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 내용을 기록할 필요가 있음

[표 6] 접속기록 포함 내용 예시

□ 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 내부관리계획에서 관리 절차를 수립 시행

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

- 가명정보 또는 추가정보가 보조저장매체 등에 저장되어 있는 경우 잠금장치가 있는 안전한 장소에 보관하여야 하며, 이러한 보조저장매체 등에 대한 반·출입 통제를 위한 보안대책 마련

제 III 편

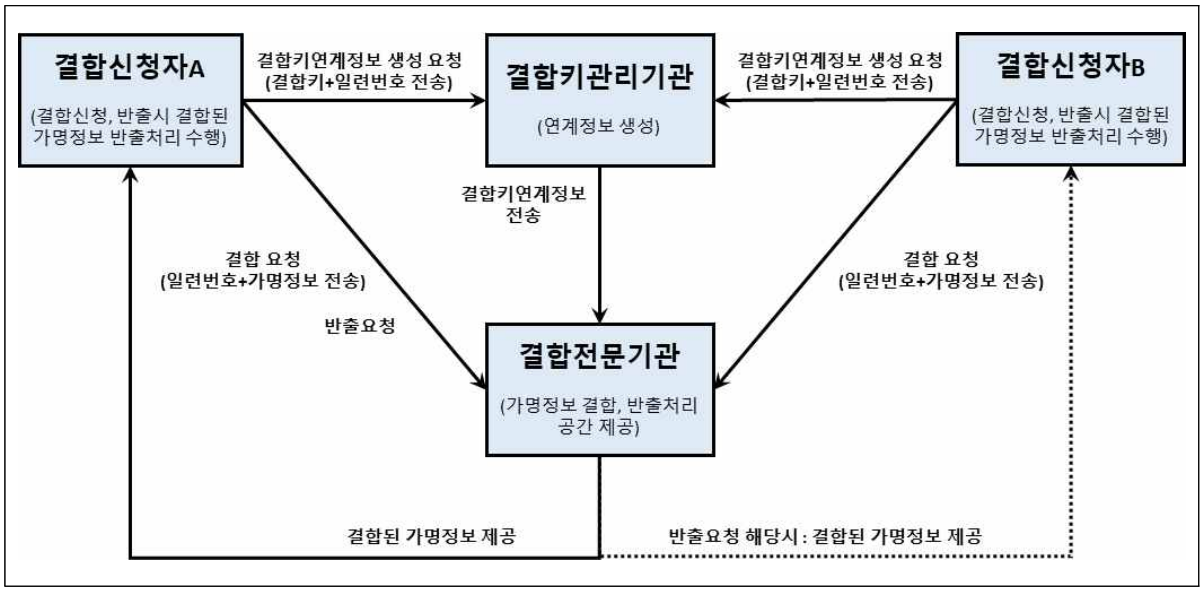
가명정보 결합

1. 가명처리 결합 · 반출
2. (참고) 가명정보 내부 결합

1 가명처리 결합·반출

□ 가명정보 결합 · 반출 절차

○ 서로 다른 개인정보처리자간의 교육분야 가명정보의 결합은 개인정보 보호위원회 또는 교육부 장관이 지정하는 결합전문기관을 통해 수행



<그림 7> 결합전문기관을 통한 가명정보 결합 개념도

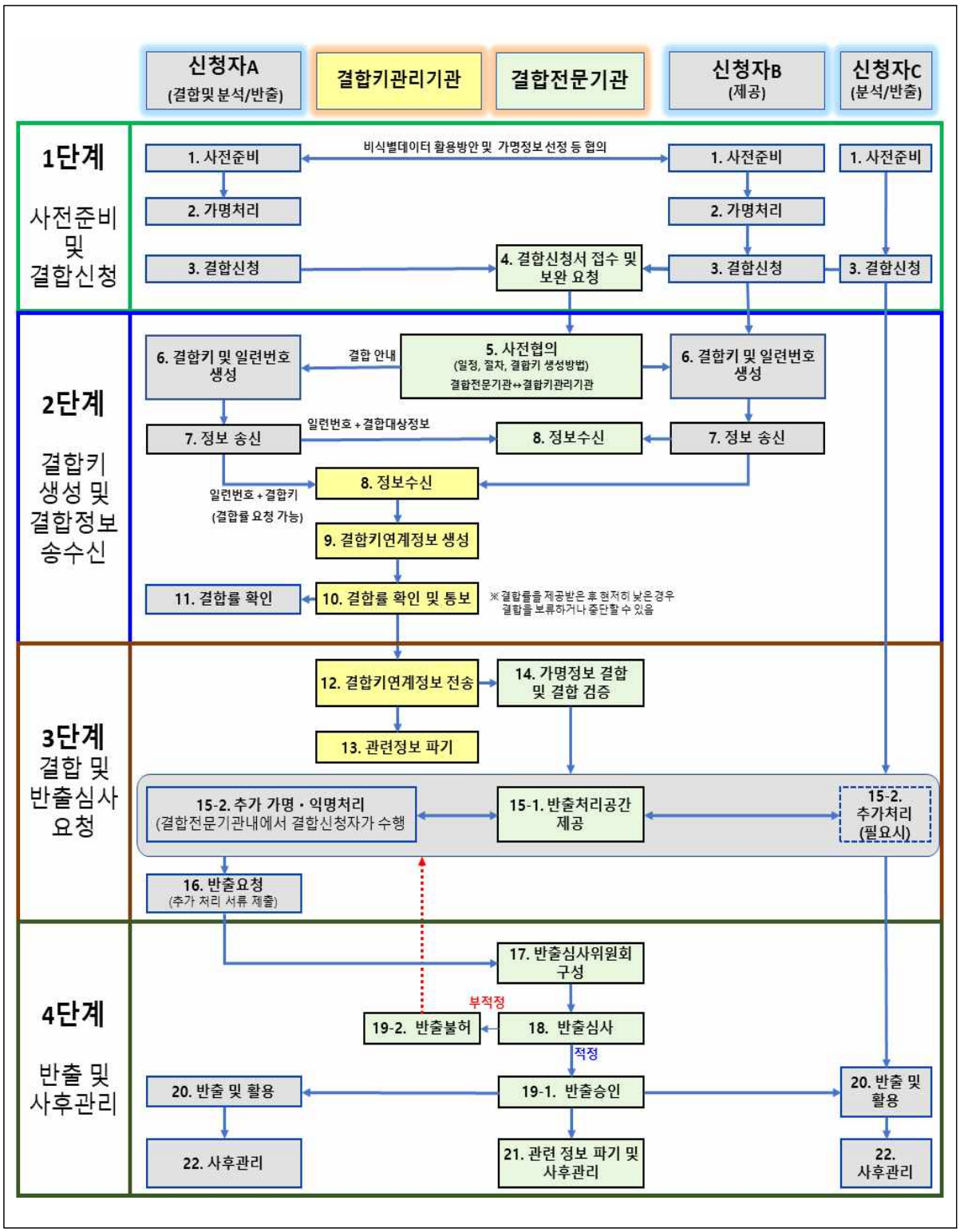
[가명정보 결합 기관 및 대상 예시]

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)

□ 가명정보 결합 · 반출 세부 절차



<그림 8> 결합전문기관을 통한 가명정보 결합 절차 예시

[단계 1 : 사전준비 및 결합신청]

1. 사전준비

○ 결합신청자 A와 B는 상호 협의*를 통해 가명정보 결합에 대한 사전준비 수행

* 결합 목적에 부합하는 가명정보 선정 및 시계열 결합 여부 확인, 결합키 생성 항목 선정, 목적을 달성하기 위해 필요한 가명처리 수준 등

○ 결합신청자들은 공통으로 보유하고 있는 정보 중에서 결합키를 생성할 때 활용할 항목을 결정해야 함

[결합키 생성 항목 정의 예시]

- 결합신청자A : 성명, 휴대전화번호, 성별, 성적
- 결합신청자B : 성명, 휴대전화번호, 교통수단, 이동시간

☞ A와 B가 동일하게 가지고 있는 성명, 휴대전화번호를 결합키 항목으로 선정

※ 결합키 생성 시 주의사항

- 결합키 생성에 사용되는 항목들에 한글이 포함되어 있는 경우 동일한 인코딩 방식을 사용하는지를 확인해야 함
  - 동일한 결합키가 생성되는지 확인하기 위해 각자 동일한 데이터에 동일한 알고리즘을 적용하여 암호화 처리 후 결과 값을 확인해야 함

    ※ EUC-KR로 인코딩 된 데이터와 UTF-8로 인코딩된 데이터를 동일한 일방향 암호화를 하는 경우 서로 다른 결과 값이 생성될 수 있음

    ☞ 결합률 0% 발생

    ※ 해시로 인코딩된 바이너리를 텍스트로 바꾸는 방법(예: Base64)을 서로 다른 방법을 사용할 경우 한글의 인코딩이 동일하더라도 결합률 0% 발생
- 데이터의 현행화 여부를 확인하여 상호 현행화할 수 있도록 해야 함

  ☞ 결합률 저하 발생

2. 가명처리

○ 결합신청자는 결합대상정보에서 정보주체별로 중복되지 않는 일련의 값(일련번호) 생성

[일련번호 생성방법 예시]

결합신청자A

일련번호	성명	전화번호	…
A1	홍길동	090-2254-4565	
A2	김철수	090-1511-2545	
A3	이영희	090-5354-9178	
…	…	…	…

결합신청자B

일련번호	성명	전화번호	…
B1	이영희	090-5354-9178	
B2	홍길동	090-2254-4565	
B3	김철수	090-1511-2545	
…	…	…	…

○ 결합신청자는 일련번호와 결합키 생성을 위한 항목을 제외한 나머지 정보들에 대해 가명처리 수행

[가명처리 대상 항목 선정 예시]

- 결합신청자A : 성명, 휴대전화번호, 성별, 성적
- 결합신청자B : 성명, 휴대전화번호, 교통수단, 이동시간

☞ A와 B가 동일하게 가지고 있는 성명, 휴대전화번호를 결합키 항목으로 선정하고 다른 항목인 성별, 성적, 교통수단, 이동시간 등이 가명처리 대상

※ 교통수단, 성별은 개인식별 가능성이 현저히 낮은 항목으로 가명처리 대상에서 제외 가능

– 가명처리 시 가명정보 처리환경을 고려하여 가명처리 수준 결정

– 결합신청자는 가명처리 수행에 대한 처리결과를 기록·보관

※ 세부 방법은 본 가이드라인 Ⅱ편 가명처리 > 2. 가명처리 세부 절차를 참조

3. 결합신청

○ 결합신청자는 ‘가명정보 결합신청서’(별지 7)를 각자 작성하고, 관련 첨부서류를 함께 준비 후 교육부 장관이 지정한 결합전문기관에 결합 신청서를 제출

※ 작성 방법은 ‘가명정보 결합신청서 작성 예시’(별지 8) 참조

4. **결합신청서 접수 및 보완요청**(결합전문기관)

○ **(결합전문기관)** 결합신청자의 신청을 접수하고 결합에 대한 타당성 검토를 실시한 후, 신청서와 첨부서류를 확인하여 미흡한 경우 부족한 서류 등에 대해 결합신청기관에 보완 요청

○ **(결합신청자)** 결합전문기관이 보완 요청한 서류 등에 대해 추가 제출하고 결합전문기관이 가명정보의 가명처리 수준에 대하여 권고하는 경우, 특별한 사정이 없으면 이를 반영

[단계 2 : 결합키 생성 및 결합정보 송수신]

5. **사전협의**(결합신청자, 결합키관리기관)

○ 결합전문기관 및 결합키관리기관은 결합신청자와 결합 및 결합키생성에 관한 사항에 대해 사전 협의 가능

※ (결합전문기관) 결합일정 및 절차, 전송 파일 형태 등 결합에 필요한 사항, (결합키관리기관) 결합키생성 관련 기술지원, 사전 결합률 확인 여부 등

6. **결합키 및 일련번호 생성**

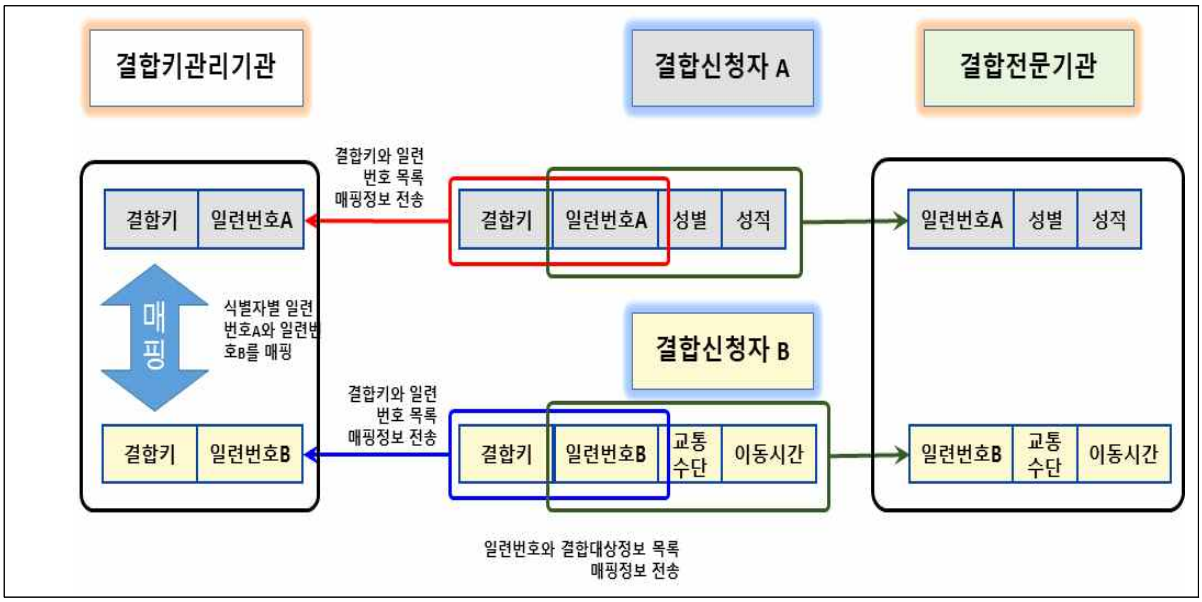
○ **(결합키 생성)** 결합신청자는 사전준비 단계에서 합의한 항목과 결합키관리기관과 합의한 사항 등을 적용하여 결합키와 일련번호를 생성

7. **정보 송신**

○ **(정보 전송)** 결합신청자는 결합키관리기관과 결합전문기관에 필요한 정보를 전송

– 생성한 결합키와 일련번호를 매핑한 정보를 결합키관리기관에 전송

– 결합전문기관이 제공하는 전송방법을 활용하여 결합전문기관에 결합대상정보와 일련번호를 전송(오프라인 포함)



<그림 9> 결합키 생성 및 결합용 관련 정보 전송 예시

– 결합신청자는 결합에 필요한 정보를 암호화 등 안전한 방법으로 결합전문기관 및 결합키관리기관에 전송

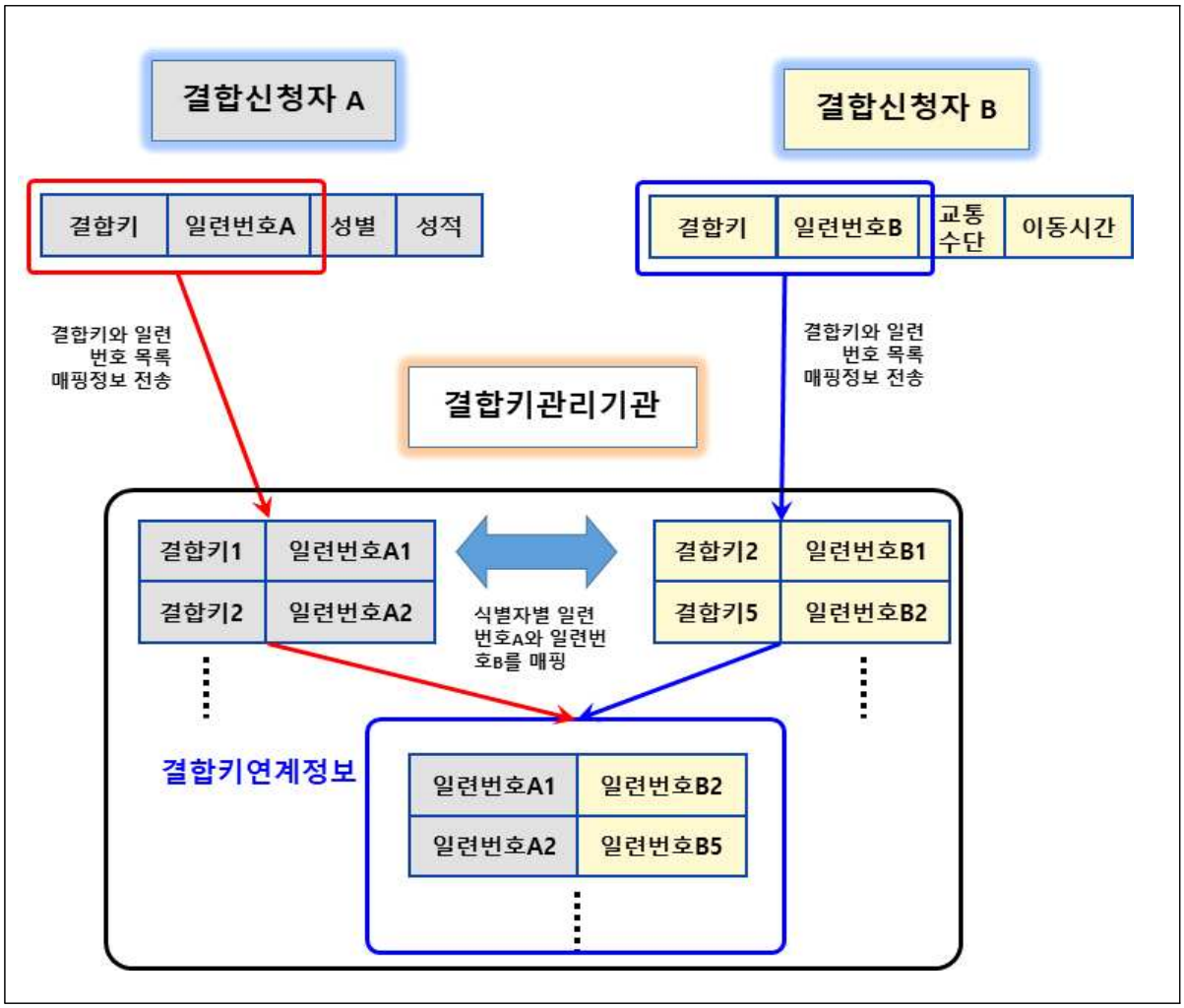
※ 정보통신망을 통하여 송·수신하거나 보조저장매체 등을 통해 전송하는 경우, 압축 및 암호화, 무결성 검증 등은 결합전문기관에서 제공하는 방법과 절차를 준수

8. 정보 수신(결합전문기관, 결합키관리기관)

○ 결합전문기관과 결합키관리기관은 결합신청자가 전송한 정보 수신

9. 결합키연계정보 생성(결합키관리기관)

○ 결합키관리기관은 결합신청자로부터 받은 '결합키+일련번호'를 기반으로 결합키연계정보 생성



<그림 10> 결합키연계정보 생성

10. 결합률 확인 및 통보(결합키관리기관)

○ 결합신청자가 결합키관리기관과의 협의 단계에서 사전결합률 확인을 요청한 경우, 결합키관리기관은 결합키연계정보 생성과정에서 결합률을 확인하여 통보

11. 결합률 확인

○ 결합신청자는 결합률을 확인한 후 필요한 경우 결합키를 재생성하거나 결합신청 자체 중단 가능

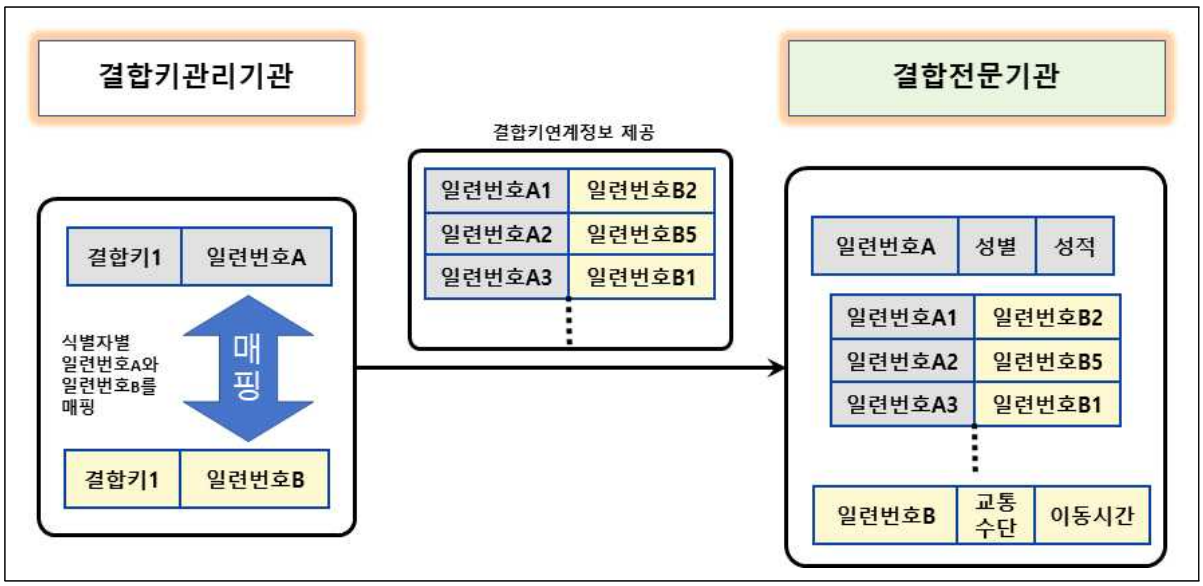
- 결합키에 문제(결합률 0% 등)가 있다고 판단하거나 효율성이 높은 가명정보 결합을 위해 결합키 생성 항목을 변경하는 경우 등

○ 단순히 결합키 생성 항목만 변경하는 경우 결합신청 절차를 생략할 수 있으나, 결합신청 내용의 변경(결합 목적, 항목수, 레코드 수 등)이 있는 경우 결합신청을 다시 해야 함

[단계 3 : 결합 및 반출심사 요청]

12. 결합키연계정보 전송(결합키관리기관)

○ 결합전문기관에게 결합을 위한 결합키연계정보 전송



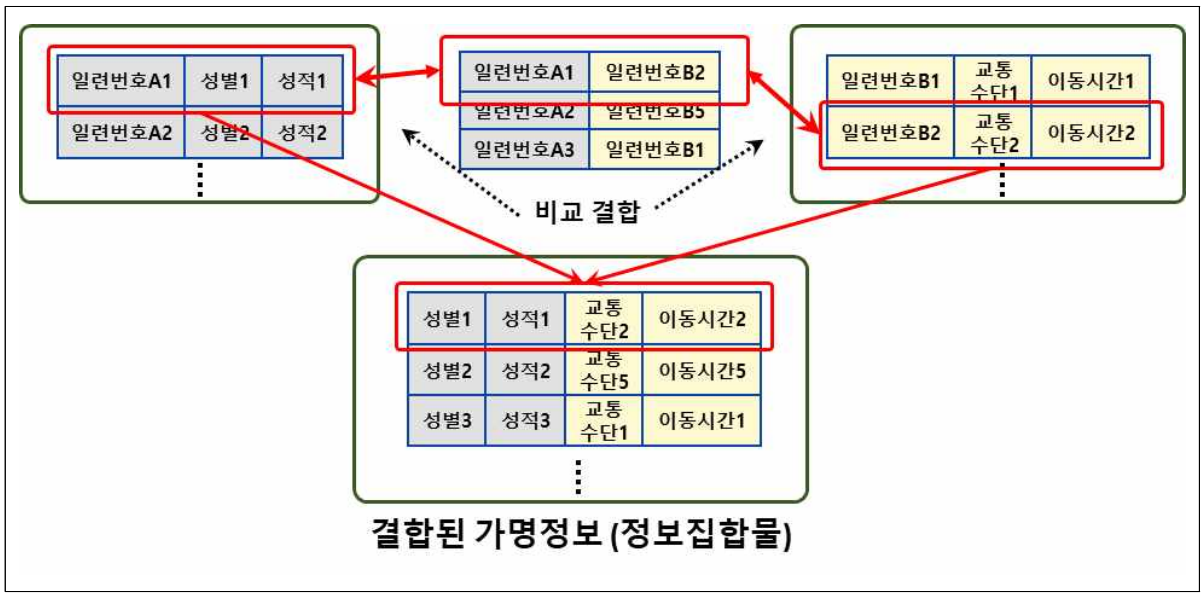
<그림 11> 결합키연계정보 전송 예시

13. 관련정보 파기(결합키관리기관)

○ 결합키연계정보가 결합완료(반출이후) 등 더 이상 불필요한 경우 즉시 파기

14. 가명정보 결합 및 결합 검증(결합전문기관)

○ 결합신청자로부터 제공받은 가명정보를 결합키관리기관으로부터 받은 결합키연계정보와 비교하여 결합을 수행하고, 결합 후에는 결합된 가명정보에 대한 무결성 등 결합에 대한 검증 실시



<그림 12> 결합키연계정보를 이용한 가명정보 결합 예시

15-1. 반출처리공간 제공(결합전문기관)

○ 결합신청자가 결합된 가명정보 반출을 위해 추가적인 가명처리 및 익명처리를 할 수 있도록 반출처리공간 제공

※ 결합된 정보를 분석할 수 있는 시설, 장비 등 시설을 구비한 경우 결합된 정보를 결합전문기관 내에서 분석하고 분석결과물만 반출할 수 있음

15-2. 반출을 위한 추가 가명·익명처리

○ 결합신청자는 결합된 정보를 결합전문기관 내에 설치된 반출처리공간에서 반출을 위한 추가 가명·익명처리를 해야 하며, 결합전문기관에 자문 등 필요한 지원 요청 가능

- 이때, 추가 가명처리를 할 수 있는 자는 결합신청자 중에서 결합된 정보를 반출하여 활용하고자 하는 자로 제한됨

○ 반출심사는 결합된 정보를 반출할 자의 처리 목적과 처리환경 등을 고려하여 이루어지므로, 추가 가명·익명처리 시 처리 수준은 결합된 정보를 활용하고자 하는 자의 처리환경 등을 고려하여 판단

○ 익명정보로도 목적 달성이 가능한 경우, 익명처리하여 반출

16. 반출요청

○ 결합신청자는 반출을 위한 추가처리가 완료되었다고 판단한 경우 결합전문기관에서 정한 규정에 따라 반출 요청

- 반출 요구 시 결합신청자는 반출 요구 조건에 충족하도록 추가적으로 수행한 가명·익명처리 등 관련 서류 제출
- 반출심사는 결합신청자별로 이루어지므로 추가처리가 완료되는 즉시 개별적으로 결합전문기관에 반출을 요청

[단계 4 : 반출 및 사후관리]

17. 반출심사위원회 구성(결합전문기관)

○ 결합전문기관은 결합신청자가 반출을 요청하는 경우 지체 없이 반출심사위원회를 구성하여 반출 여부를 심사

- 반출심사위원회 구성은 개인정보 보호에 관하여 경험과 학식이 풍부한 사람으로서 다음 각 호에 해당하는 사람을 고루 포함하여 3인 이상 7인 이내의 위원으로 구성

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 보호와 관련한 경력과 전문성이 있는 사람

- 결합신청자는 반출요청을 한 경우 심사에 필요한 사항을 제출하고 이를 설명해야 함
- 결합신청기관의 임직원 등 이해관계자는 반출심사위원회 위원으로 참여 불가

18. 반출심사 : 반출 승인과 반출불허(결합전문기관)

○ 결합신청자가 반출심사를 위해 필요하다고 판단하거나 반출심사위원회의 요청이 있는 경우, 추가자료를 제출하거나 관련된 내용을 반출심사위원회에 출석하여 설명해야 함

- 결합신청자가 결합에 사용된 가명정보를 제공한 개인정보처리자인 경우 해당 정보와의 결합가능성 등이 반출승인 과정에서 고려될 수 있음
- 심사를 득하지 못한 경우 결합신청자와 협의 하에 재처리를 요구하거나 반출심사 종결

※ 이 경우에도 반출승인을 위하여 결합전문기관에 자문 등 필요한 지원을 요청할 수 있음

19-1. 반출승인

○ 결합전문기관은 반출심사 “적정”시 반출요청을 승인하여 결합 및 추가 처리된 정보 반출

19-2. 반출불허

○ 결합전문기관은 반출심사 “부적정”시 반출요청을 불허하고 추가 가명·익명처리를 요구

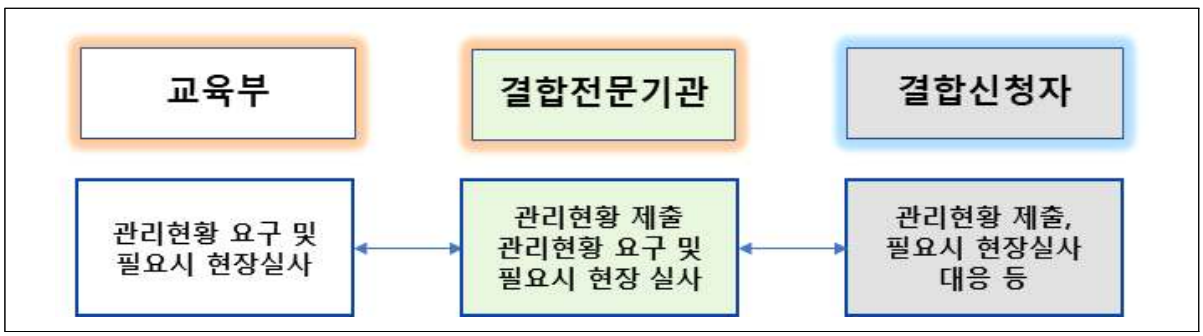
20. 반출 및 활용

○ 결합신청자는 반출된 정보를 결합 목적에 맞게 활용 가능

21. 관련 정보 파기 및 사후관리(결합전문기관)

○ **(결합 이력 관리)** 결합이 종료되면 관련 이력을 관리하고 법령에서 별도로 보유하도록 한 정보를 제외하고 즉시 삭제처리(결합키 등)

○ **(사후관리)** 결합신청자에 대한 사후관리 및 감독을 실시하며, 이 경우 사후관리 및 감독을 위해 결합전문기관이 요청한 자료 등에 대해 결합신청자는 특별한 사유가 없으면 응해야 함



<그림 13> 결합전문기관의 관리현황 조사요구와 대응

21. 사후관리

○ 결합신청자는 활용에 따른 자체 모니터링 및 사후관리에 대해 본 가이드라인 ‘Ⅱ편 가명처리 > 2-4. 가명처리 사후관리’에서 기술하고 있는 내용에 따라 관리를 해야 함

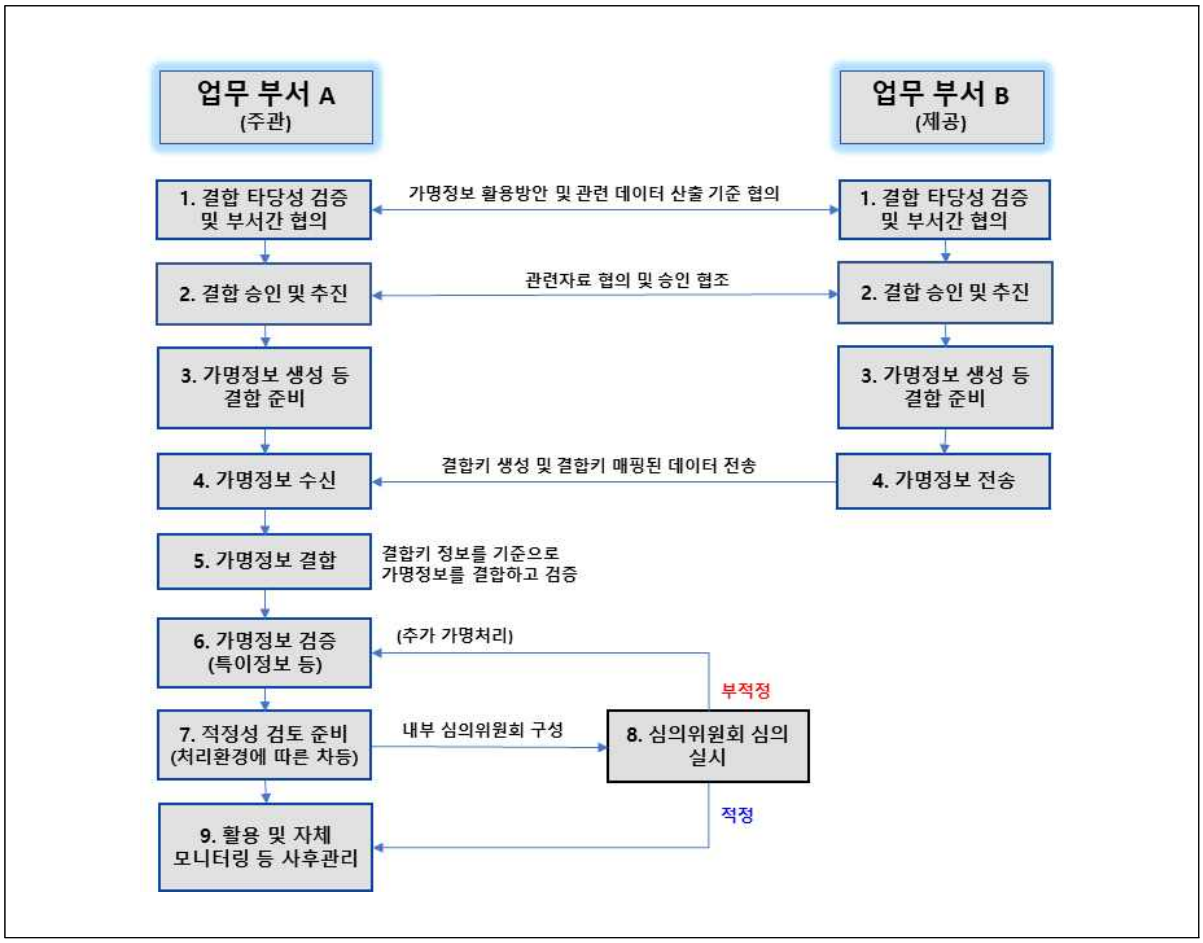
2 (참고) 가명정보 내부 결합

○ 개인정보처리자가 보유한 개인정보를 내부에서 가명처리하여 결합을 하는 경우 별도의 외부 결합전문기관을 거치지 않음

– 결합을 수행할 부서에서 결합할 가명정보를 모두 제공받아 결합키를 이용하여 자체적으로 결합 수행

○ 안전한 결합을 위하여 결합전문기관의 결합절차(Ⅲ편 1. 가명처리 결합·반출)와 유사하게 처리하는 것을 권고

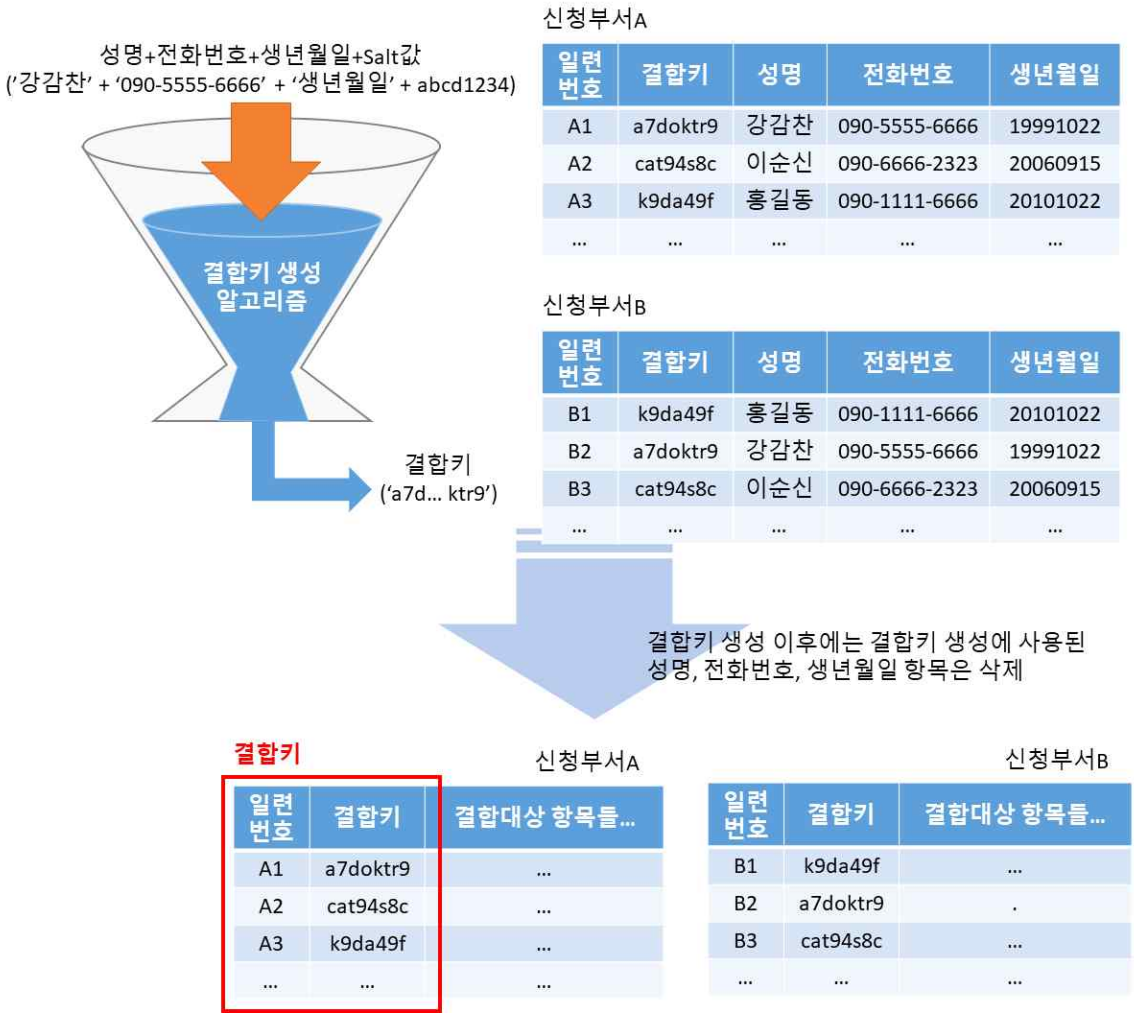
– 내부 결합에 대하여는 법령에서 별도로 정하고 있지 않지만, 결합 과정에서 가명정보가 재식별되지 않도록 유의



<그림 14> 자체 가명정보 결합 절차 예시

< 결합키 생성 방법 >

- 결합키 생성을 위해서는 생성에 필요한 사항 및 결합에 관련된 사항을 관련 부서와 사전 협의해야 함
  - 결합키는 사전준비 단계에서 부서 간 합의한 항목과 Salt값 등을 적용하여 생성



일련번호	결합키	성명	전화번호	생년월일
A1	a7doktr9	강감찬	090-5555-6666	19991022
A2	cat94s8c	이순신	090-6666-2323	20060915
A3	k9da49f	홍길동	090-1111-6666	20101022
...	...	...	...	...

일련번호	결합키	성명	전화번호	생년월일
B1	k9da49f	홍길동	090-1111-6666	20101022
B2	a7doktr9	강감찬	090-5555-6666	19991022
B3	cat94s8c	이순신	090-6666-2323	20060915
...	...	...	...	...

일련번호	결합키	결합대상 항목들...
A1	a7doktr9	...
A2	cat94s8c	...
A3	k9da49f	...
...	...	...

일련번호	결합키	결합대상 항목들...
B1	k9da49f	...
B2	a7doktr9	.
B3	cat94s8c	...
...	...	...

<그림 15> 결합키 생성 예시

- 결합을 위한 식별정보의 가명처리에 사용하는 기법은 일반적으로 일방향 암호화를 사용
- 일방향 암호화를 사용할 때는 국내 권고기준인 해시 알고리즘 SHA-256 이상 사용을 권고

○ 결합용 가명정보를 생성한 부서는 결합을 수행할 부서(주관)로 해당 가명정보를 전송(이동)하고, 전송 시 가명정보 안전성 확보 조치 기준에 따른 안전성을 확보

○ 결합을 수행할 부서(주관)는 결합키*를 기반으로 서로 다른 부서에서 받은 가명정보와 보유하고 있는 가명정보를 결합하고 결합된 가명정보에 대한 무결성 검증

* 결합방식에 따라 결합키 단독으로 결합을 하거나 결합키와 일련번호를 매핑한 결합키연계정보를 활용하여 결합할 수 있으며 결합의 방식은 기관의 선택에 따라 달리 할 수 있음

- 가명정보 결합과 관련된 정보(결합키 등)는 가명정보의 결합 및 적정성 검토가 완료되는 즉시 삭제
- 가명정보처리자는 결합된 가명정보를 처리하고자 하는 경우 별도의 안전한 장소에서 최소한의 권한이 부여된 최소한의 인원을 지정하여 운영
- 제한구역 이상의 안전한 공간에서 가명정보를 처리

※ 결합된 가명정보와 원본 개인정보를 동시에 취급하는 자가 없도록 권한 및 직무분리

○ 결합한 정보에 대해 결합된 가명정보의 처리 수준이 적정한지 판단하고 필요한 경우 추가 가명처리 수행

제 Ⅳ 편

익명처리

1 개 요

❖ 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 익명처리해야 함

○ 익명처리 업무를 수행하는 자는 익명처리 대상 개인정보를 처리하는 업무 수행 금지. 다만, 불가피한 사유가 있을 경우 보완통제 대책을 수립하여 관리자의 승인 하에 제한적으로 취급 가능

○ 개인정보처리자는 익명정보 적정성 검토를 수행하는 경우 가명정보 적정성 검토 위원회와 동일한 수준으로 구성 운영

○ 익명정보처리자는 '익명정보 관리대장'(별지 6)을 기록·관리하고 개인정보처리자는 년 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

○ 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 사전 필터링
- 이미 개방한 데이터가 다른 정보와 결합하여 개인 식별이 가능한지 여부 등을 주기적으로 모니터링한 후 재식별이 되는 경우 해당 개인정보 삭제 또는 익명처리

※『공공데이터의 제공 및 이용 활성화에 관한 법률』,『공공데이터 관리지침』에 명시된 개인정보 등 비공개 대상정보의 포함여부 확인 절차를 준수해야 함

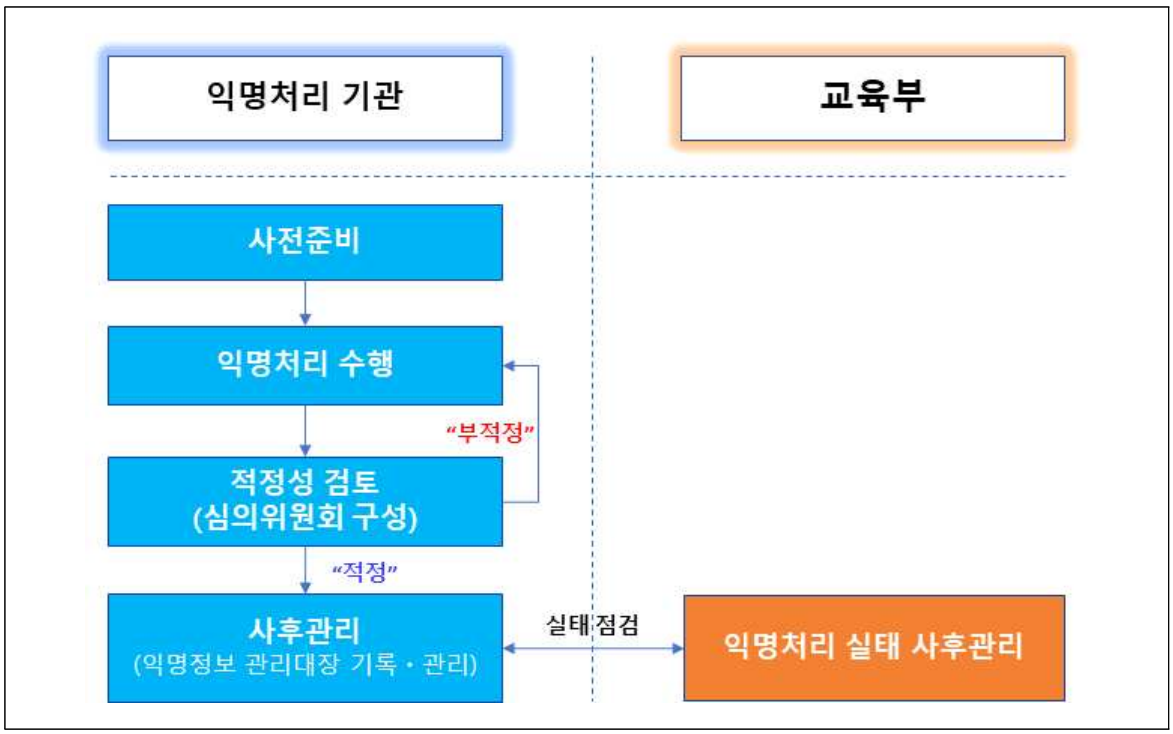
익명정보 재식별 위험과 적정성 충족 여부에 대한 책임성

- 개인정보는 가명·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	추론가능성	연결가능성
가명정보	없음	없음	존재	존재	존재
익명정보	없음	없음	없음	없음	없음

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

□ 익명처리 절차 개념도



<그림 16> 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

○ (**사후관리**) 익명처리된 익명정보에 대해 기록·관리하고 재식별 발생 시 대응할 수 있도록 대책 수립 가능

○ (**익명처리 실태 사후관리**) 익명처리 기록·관리 등에 관한 사항을 조사 및 점검 실시

□ 익명처리 예시

[개인정보와 속성자 특징]

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
〃	〃	〃	〃	〃	〃	〃	〃

[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	〃
〃	〃	〃	〃	〃	〃

성별	혈액형		전공	학위	통계
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
〃	〃		〃	〃	〃

· 성별/혈액형별 전공과 학위 현황의 익명정보를 만들겠다는 목적으로 프라이버시 보호모델 k-익명성* 값은 30 이상으로 설정

* k-익명성이란 동일한 속성 또는 속성의 조합을 가지는 레코드가 최소한 k개 이상 존재하도록 하여 프라이버시를 보호하는 모델을 말함

· '성명', '연락처'는 특정 개인이 식별 가능하므로 삭제 처리

· '성별'은 활용 목적에 필요한 속성자이므로 유지

· '생년월일'은 활용 목적에 필요한 속성자가 아니므로 삭제

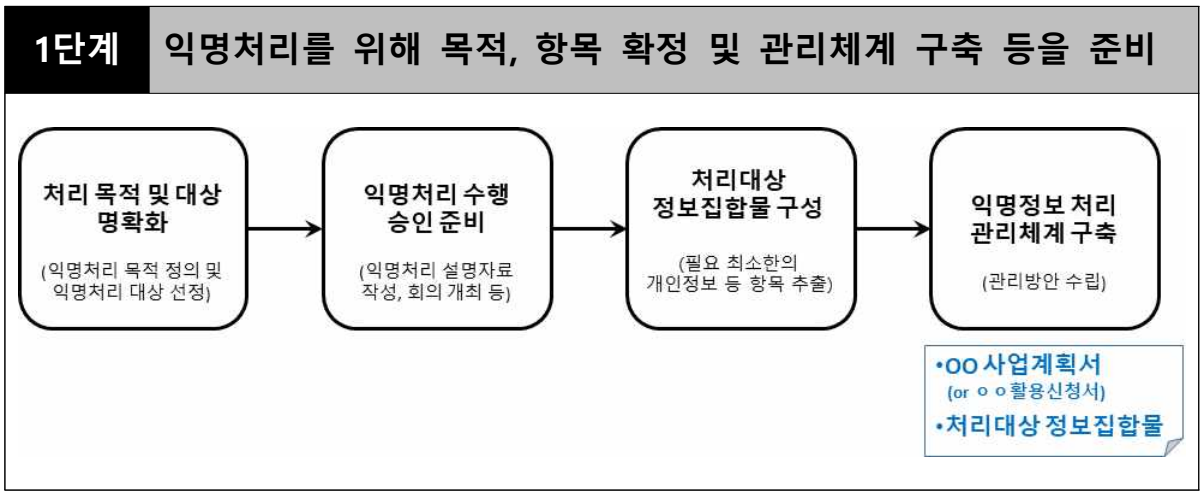
· '혈액형'은 활용 목적에 필요한 속성자이므로 유지. 다만, Rh-의 경우 희귀 혈액형 유형으로 개인이 식별될 가능성이 있는 경우 해당 레코드 삭제

※ 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 속성 정보이므로 유지. 다만, 개인이 식별될 가능성이 있는 경우 k-익명성에서의 k값은 30 이상이 나오도록 범주화하여 통계처리

2 익명처리 세부 절차

2-1 사전준비 (1단계)



<그림 17> 익명처리 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

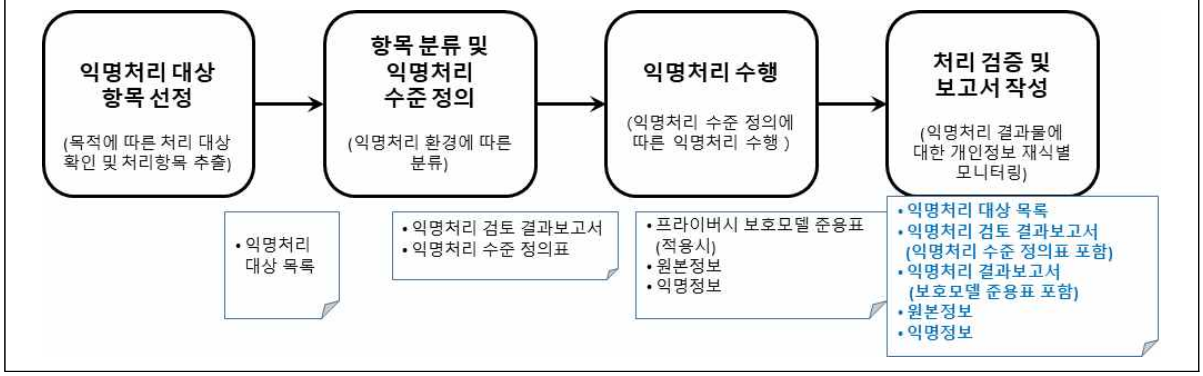
* 익명정보 관리대장 기록 및 관리자 지정 등에 관한 사항을 계획에 포함 가능

주요 산출물

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

2-2 익명처리 수행 (2단계)

2단계 목적, 위험도 등을 고려하여 정보집합물에 대한 가명처리 수행



<그림 18> 익명처리 수행 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

□ 항목 분류 및 익명처리 수준 정의

○ **(항목 분류 및 검토 결과보고서 작성)** 개인정보 항목별 위험도 분류표 구성과 항목별 위험도 분류

– 식별가능성이 있거나 복원가능성이 있는 항목은 삭제하여 항목별 위험도 분류 대상에서 제외하고 기타 항목에 대해 재식별 위험 특성별 위험도 분류

[항목별 위험도 분류 예시]

· ㅇㅇ교육청이 A부서의 개인정보를 익명처리하여 홈페이지 상에 정책 통계 자료로 공개할 경우

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

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

· 항목별로 재식별 위험을 매칭하여 위험도를 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

– 항목별 위험도 분류를 고려하여 ‘익명처리 검토 결과보고서’ 작성(별지 3 참조)

2. 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	프라이버시모델 익명성 k = 100 이상
특정가능성	중	프라이버시모델 익명성 k = 50 이상
특정가능성	하	프라이버시모델 익명성 k = 20 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 ‘익명처리 검토 결과보고서’(별지 3) 등을 종합적으로 고려하여 ‘익명처리 수준 정의표’(별지 4) 작성

– 항목별 재식별 위험뿐만 아니라 전체 항목의 재식별 위험도를 고려하여 ‘익명처리 수준 정의표’에 반영

※ 가장 높은 재식별 위험에 맞추어 수준 정의가 필요한 경우 등

□ 익명처리 수행

○ **(익명처리 수행 원칙)** 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 식별되는 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』> '참고자료 2. 특이정보 정의 및 처리사례'를 참조하여 처리

- 특이정보를 처리하는 과정에서 변경사항 발생 시 필요한 경우 기존에 작성된 '익명처리 검토 결과보고서'(별지 3) 또는 '익명처리 수준 정의표'(별지 4)에 해당 내용 반영
- 적정성 검토 결과 "부적정"판정을 받은 경우 추가 익명처리 수행

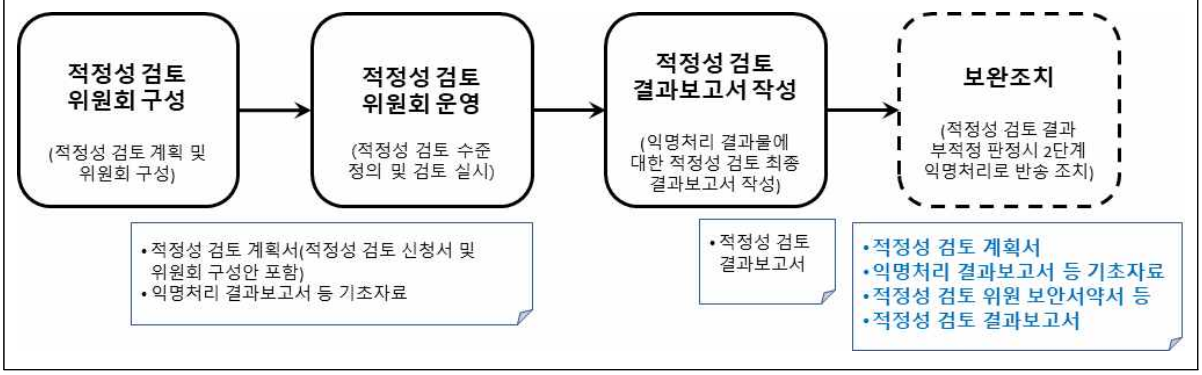
○ **(익명처리 결과보고서 작성)** 개인정보 재식별 검증 결과 재식별 가능성이 없는 경우 적정성 검토를 위한 '익명처리 결과보고서'(기관별 자유양식)를 작성

주요 산출물

- 익명처리 검토 결과보고서
- 익명처리 수준 정의표
- 익명처리 결과보고서

2-3 적정성 검토 (3단계)

3단계 익명처리 결과물에 대한 적정성 여부를 판단



<그림 19> 익명처리 적정성 검토 단계 세부 절차

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

– 익명정보 처리에 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 보호 모델을 추가하여 적정성 검토 수행 가능

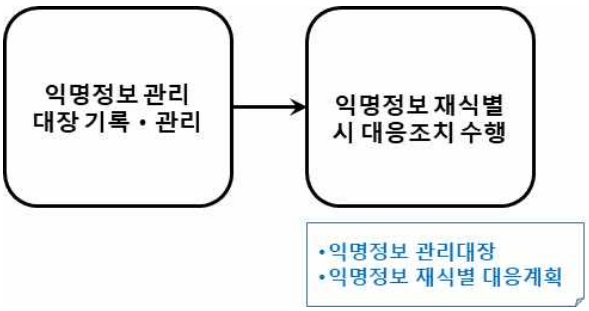
※ 단, 익명정보를 교육분야 각급기관 이외에 제공하는 경우에는 적정성 검토를 위한 위원회 구성 시 외부 위원을 과반수 이상 포함 구성

주요 산출물

- 익명처리 적정성 검토 계획서(구성안 포함)
- 익명처리 결과보고서 등 기초자료
- 보안서약서
- 익명처리 적정성 검토 결과보고서 (기관 자유양식)

2-4 사후관리 (4단계)

4단계 익명처리된 익명정보를 기록 및 관리



<그림 20> 익명처리 사후관리 단계 세부 절차

○ **(기록 관리)** 익명정보처리자는 익명정보 처리에 관한 내용*을 기록(별지 6)으로 작성하고 안전하게 보관·관리

* 익명처리 기간, 항목, 사유 및 근거, 제공받는 자(해당시), 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 시 대응조치)** 익명정보처리자는 익명정보 재식별 사고 발생 시 후속조치를 수행

– 익명정보 재식별 사고 발생 시 수행 내용

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

– 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 처리 관련 사후관리계획서

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

제 Ⅴ 편

기타

부록 1. 주요 산출물 및 처리방안
부록 2. 가명처리 및 익명처리 관련 양식

부록 1

주요 산출물 및 처리방안

□ 가명처리

단계		내용	산출물	처리방안
1단계	목적 및 대상	가명처리 목적 및 가명처리 대상 개인정보 선정	사업계획서 (제3자 제공시 계약서(안) 포함)	기록물 관리에 따른 보유기간 내 보관
	승인 준비	사업 설명자료 작성, 내부 회의 및 사업 추진 타당성 검토, 사업 승인 추진		
	정보집합물 구성	개인정보 항목을 선정하고 추출하여 정보집합물 구성	정보집합물	가명처리 후 삭제
	관리체계 구축	가명정보 보호대책 수립	내부관리계획, 사업계획서	준영구 보관
2단계	가명처리 대상 재선정	정보집합물에서 처리대상 및 대상별 특성을 확인하여 최소한의 항목을 추출	가명처리 대상 목록 (또는 정보집합물)	가명처리 후 삭제
	위험도 측정 및 검토보고서 작성	위험도 측정 및 위험도에 따른 가명처리 검토 결과 보고서 작성	가명처리 검토 결과 보고서 (별지 1)	가명정보 이용기간 종료 후 3년간 보관
	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)	
			가명정보	이용기간 종료 후 삭제
			추가정보	즉시 삭제 권고 (보관 시 가명정보와 분리, 삭제 시 가명정보와 같이 삭제)

단계		내용	산출물	처리방안
	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
3 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 (자유양식)	가명정보 이용기간 종료 후 3년간 보관
	보완조치	적정성 검토 결과 부적정 판정 시 가명처리로 반송 조치		
4 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)	개인정보처리 방침	준영구 보관
			내부관리계획	준영구 보관
			계약서 (해당 시)	법령에 따른 보유기간
	재식별 모니터링	가명정보를 처리 시 년 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	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 결과 보고서 작성	적정성 검토 결과보고서 (자유양식)	가명정보 이용기간 종료 후 3년간 보관
		적정성 검토 결과 부적정 판정 시 가명처리로 반송 조치		

단계		내용	산출물	처리방안
9	활용 및 사후관리	활용 및 가명정보 관리대장 기록·관리	가명정보 관리대장 (별지 5)	준영구 보관
		가명정보 등에 대한 안전성 확보 방안 수립 및 운영 (개인정보처리방침 공개, 내부 관리계획 수립 등)	개인정보처리 방침	준영구 보관
			내부관리계획	준영구 보관
		가명정보를 처리 시 년 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
1단계	목적 및 대상	익명처리 목적 및 익명처리 대상 개인정보 선정	사업계획서	기록물 관리에 따른 보유기간 내 보관
	승인 준비	사업 설명자료 작성, 내부 회의 및 사업 추진 타당성 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)	사업계획서	기록물 관리에 따른 보유기간 내 보관
2단계	익명처리 대상 재선정	정보집합물에서 처리대상 및 대상별 특성을 확인하여 최소한의 항목을 추출	익명처리 대상 목록 (또는 정보집합물)	익명처리 후 삭제
	항목분류 및 익명처리 수준 정의	개인정보 항목별 위험도 분류 및 항목별 익명처리 수준 정의	익명처리 검토 결과 보고서 (별지 3) 익명처리 수준 정의표(별지 4)	익명정보 이용기간 종료 후 3년간 보관
	익명처리 수행 및 처리 검증	익명처리 수행	익명정보	기간 종료 후 삭제
			추가정보	즉시 삭제
		특이정보 등 재식별 가능성 확인 시 추가적으로 익명처리 (보완조치 수행 시 익명처리 수준 정의표 수정 반영)	익명처리 수준정의표	익명정보 이용기간 종료 후 3년간 보관
3단계	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

단계		내용	산출물	처리방안
	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 결과 보고서 작성	적정성 검토 결과보고서 (자유양식)	익명정보 이용기간 종료 후 3년간 보관
		적정성 검토 결과 부적정 판정 시 익명처리로 반송 조치		
		위원 보안서약서 작성	보안서약서 (자유양식)	기록물 관리에 따른 보유기간 내 보관
4 단계	익명정보 처리 기록·관리	익명정보 관리대장 기록·관리	익명정보 관리대장 (별지 5)	준영구 보관
	익명정보 재식별 시 대응조치 수행	재식별 사고 발생시 대응계획 및 제3자 제공시 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

부록 2

가명처리 및 익명처리 관련 양식

[별지 1] 가명처리 검토 결과보고서 예시

가명정보 활용목적	◦ ㅇㅇ교육청이 거주지별 학생정보와 성적 정보들을 가명처리하여 A기관에 제공하여, 코로나로 원격학습에 따른 지역별 학업 성취도 격차를 파악하기 위한 연구 수행	
가명정보 항목	◦ 학생개인번호, 과목, 학년, 성별, 성적(점수), 시도, 시군구, 읍면동, 지번, 거주지 유형 ※ 항목을 나열하지 못하는 경우 '별지'로 추가하여 사용 가능	
처리(제공) 환경 검토	처리 환경	◦ 특정 제3자(A기관) 제공 ◦ ㅇㅇ교육청은 A기관과 교육분야 가명·익명정보 처리 가이드라인에 따라 필요한 항목들이 모두 포함된 계약체결을 통해 가명정보를 제공
	제공 받는 자의 보호 수준	◦ A기관은 개인정보처리시스템에 대한 ISMS-P 인증을 취득하고 있으며, 새롭게 가명정보처리시스템에 대해 ISMS-P 인증을 진행하고 있어 보호수준이 상대적으로 높음 ◦ 내부관리를 통해 관리적·기술적·물리적 보호조치를 수행하고 있음
	재식별 수준	◦ 가명정보를 제공받은 A기관은 학생 관련 다른 (개인)정보들을 보유하고 있지 않음
항목별 위험도 분석	◦ 학생개인번호, 학생성적정보(과목, 학년, 성별, 성적)가 결합할 경우 식별가능정보 및 특이정보 가능성 존재 ◦ '지번'은 식별가능정보 ※ 필요시 '별지'에 위험도 분석 결과 기술 가능	
최종 검토의견*	◦ 해당 연구는 특정 제3자와의 계약서 체결을 통해 가명정보를 활용하는 경우에 해당하며, 제공받는 자가 별도의 다른 (개인)정보를 통해 가명정보를 재식별 할 가능성이 낮음 ◦ 학생개인번호는 그 자체로 또는 결합시 식별될 가능성이 매우 높으므로 반드시 필요하지 않은 경우 삭제하고 과목별, 학년별 성적 추적을 위해 필요한 경우 학생개인정보를 그대로 사용하지 않도록 가명처리 필요 ◦ 학생성적정보는 결합시 식별될 가능성이 높으므로 반드시 필요한 경우가 아니라면 특정 항목은 삭제 필요. 다만, 목적달성에 필요한 경우에 한하여 최소한 k-익명성 k 값을 10 이상으로 하여 처리 ※ '성적(점수)'는 특이정보 가능성이 존재하므로 범주화 등의 가명처리가 필요 ◦ '지번'의 경우 다른(공개된 정보 등) 정보를 통해 재식별 가능성이 있어 삭제 또는 목적 달성에 필요한 경우 가명처리 필요 ◦ 그 외의 정보들은 재식별 가능성이 낮으며 목적달성을 위해 필요하다고 판단되므로 가명처리하지 않음	

* 최종 검토의견은 외부전문가를 활용하여 자문 및 작성을 요청할 수 있음

[별지 2] 가명처리 수준 정의표 예시

○ '가명처리 검토 결과보고서'에 분류한 개인정보에 대한 가명처리 수준 정의

순번	항목명	처리수준	비고
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] 익명처리 검토 결과보고서 예시

<table>
<tr><td>익명정보
활용목적</td><td colspan="2">◦ ㅇㅇ교육청은 학생의 과목, 학년, 성별, 성적을 익명처리하여 학부모에게 해당 정보를 공개하여 과목별/학년별/성별 성적 분포도를 제공하고자 함</td></tr>
<tr><td>익명정보
항목</td><td colspan="2">◦ 학생개인번호, 과목, 학년, 성별, 성적(점수)
※ 항목을 나열하지 못하는 경우 '별지'로 추가하여 사용 가능</td></tr>
<tr><td rowspan="3">처리(제공)
환경 검토</td><td>처리 환경</td><td>◦ 외부 공개</td></tr>
<tr><td>제공 받는
자의 환경</td><td>◦ 불특정 다수의 환경</td></tr>
<tr><td>제공 받는
자의 보호
수준</td><td>◦ 보호 수준 없음</td></tr>
<tr><td rowspan="3">항목별
위험도
분석</td><td>특정
가능성</td><td>◦ 학생개인정보 및 지번은 개인을 명확하게 알아볼 수 있음
◦ 학년, 과목, 성별, 성적의 결합은 특성 집합을 관찰하여 개인을 알아볼 가능성이 존재 등등</td></tr>
<tr><td>추론
가능성</td><td>◦ 특정 과목, 특이 성적의 결합은 무시할 수 없는 확률로 추론하여 개인을 알아볼 가능성 존재 등등</td></tr>
<tr><td>연결
가능성</td><td>◦ 모든 항목들의 일반화가 부족할 경우 외부 공개된 정보와 연결하여 개인을 알아볼 가능성이 존재 등등</td></tr>
<tr><td>최종
검토의견*</td><td colspan="2">◦ 해당 정보는 불특정 다수에게 제공하는 외부 공개에 해당하며, 제공받는 자가 별도의 다른 (개인)정보를 통해 가명정보 재식별을 시도할 가능성이 매우 높음
◦ 과목, 학년, 성별, 성적 결합시 특이정보에 따라 식별될 가능성이 높으므로 반드시 일반화의 강도를 높여서 처리해야 함. 최소한 k-익명성 k 값을 50 이상으로 하여 처리
※ '성적(점수)'는 특이정보 가능성이 존재하므로 범주화 등의 가명처리가 필요
※ '과목'은 특이정보 가능성이 존재하므로 가명처리가 필요
◦ '학생개인번호', '시도',' 시군구', '읍면동', '거주지 유형', '지번'의 경우 다른(공개된 정보 등) 정보를 통해 재식별 가능성 및 목적 달성에 불필요하므로 삭제 필요</td></tr>
</table>

* 최종 검토의견은 외부전문가를 활용하여 자문 및 작성을 요청할 수 있음

[별지 4] 익명처리 수준 정의표 예시

○ '익명처리 검토 결과보고서'에 분류한 개인정보에 대한 가명처리 수준 정의

- ㅇㅇ교육청 과목별/학년별/성별 성적 현황

순번	항목명	처리수준	비고
1	학생개인번호	◦ 익명처리(삭제)	◦ 학생개인번호 정보는 분석 목적에 필요하지 않음
2	과목	◦ 익명처리(범주화)	◦ 처리하지 않는 항목을 작성 (과목, 성별 등이 결합하여 특이정보가 발생할 경우 삭제 등의 가명처리 필요)
3	학년		
4	성별		
5	성적(점수)	◦ 익명처리 (일반화 : 100점 만점 기준으로 5점 단위, 60점 미만 삭제 및 95점 이상은 90~100점으로 일반화)	◦ 특이정보 발생시 일반화 기준 상향 필요
6	시도	◦ 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

순번	기간	목적	항목	처리 및 보유기간	제공받는 자 등	위탁 사항	제한사항	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.
   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 : 추가정보의 경우 가명정보 생성즉시 파기 후 '추가정보 동시 파기' 작성 및 기타 추가적인 사항에 대해 이 란에 작성한다.
11. 가명처리를 수행한 자 : 가명처리를 수행한 자의 이름을 작성하고 서명한다.
12. 책임자 : 가명정보 처리 책임자 이름을 작성하고 서명한다. (ex. 가명처리 부서의 책임자)

[별지 6] 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.
4. 항목 : 익명정보의 항목을 작성한다.
5. 사유/근거 : 익명정보 처리 사유 및 근거를 작성한다.
6. 제공받은 자 : 익명정보를 제공한 경우 제공받은 자의 정보를 작성한다.

   ※ 예시) 기업명 또는 성명, 담당자 연락처
7. 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
8. 기타 : 익명정보 재식별시 파기 여부 등 추가적으로 필요한 내용을 작성한다.
9. 익명처리를 수행한 자 : 익명처리를 수행한 자의 이름을 작성하고 서명한다.
10. 책임자 : 익명처리 책임자의 이름을 작성하고 서명한다.

[별지 7] 가명정보 결합신청서

가명정보 결합 신청서

신청번호	

결합신청자			
기관명		사업자등록번호 또는 법인등록번호	
주소		대표자명	
담당자		담당자 연락처 (전화, e-mail)	
신청자 구분	[ ] 개인 [ ] 공공기관 [ ] 비영리법인 [ ] 민간기관		

가명정보 제공		해당없음 [ ]
파일명		
제공방법	[ ] 온라인 [ ] 오프라인	
제출예정일	년 월 일	
전체 가명정보 제공 기관명(총수)		
제공정보 요약	컬럼 수	
	전체 레코드 수	
	전체 파일 크기	

결합 결과물 이용		해당없음 [ ]
시계열 분석	[ ] 해당없음 [ ] 시계열(신규) [ ] 시계열(추가, 결합접수번호 :)	
결합목적	[ ] 통계작성 [ ] 과학적 연구 [ ] 공익적 기록보존 등	
세부결합목적		

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

년 월 일

신청인 (서명 또는 인)

결합전문기관의 장 귀하

첨부 서류	1. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류 1부 2. 결합 대상 가명정보에 관한 서류(전체 항목명 가명처리 대상 항목명, 가명처리 기법 및 예시 등) 1부(해당 경우에 한함) * 결합키 생성에 사용된 속성 제외 3. 결합 목적을 증명할 수 있는 서류 1부 4. 안전조치계획 및 이를 증빙할 수 있는 서류 1부

[별지 8] 가명정보 결합신청서 작성 예시

☞ 개인 홍길동과 신청기관 A사와 신청기관 B사가 신청하는 경우

[개인정보처리자 개인 홍길동의 신청서 예시]

가명정보 결합 신청서

신청번호	A-2020-10-001

결합신청자			
기관명	해당없음	사업자등록번호 또는 법인등록번호	1976년 10월 10일
주소	서울시 강남구 강남대로 2길 ㅇㅇ	대표자명	해당없음
담당자	홍길동	담당자 연락처 (전화, e-mail)	010-123-1234 abc@cdefg.com
신청자 구분	[√] 개인 [ ] 공공기관 [ ] 비영리법인 [ ] 민간기관		

가명정보 제공		해당없음 [ ]
파일명	2019년도_종합	
제공방법	[√] 온라인 [ ] 오프라인	
제출예정일	2020 년 10 월 22 일	
전체 가명정보 제공 기관명(총수)	총 2개 : 홍길동(2019년도_종합), 결합신청기관 A사(파일명1) ※ 결합신청기관 B사는 별도의 가명정보를 제공하지 않고 활용만 함	
제공정보 요약	컬럼 수	25개
	전체 레코드 수	10,500개
	전체 파일 크기	25 MB

결합 결과물 이용	해당없음 [√]
시계열 분석	[ ] 해당없음 [ ] 시계열(신규) [ ] 시계열(추가, 결합접수번호 :)
결합목적	[ ] 통계작성 [ ] 과학적 연구 [ ] 공익적 기록보존 등
세부결합목적	

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

2020 년 10 월 22 일

신청인 홍 길 동 (서명 또는 인)

결합전문기관의 장 귀하

첨부 서류
1. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류 1부 2. 결합 대상 가명정보에 관한 서류(전체 항목명 가명처리 대상 항목명, 가명처리 기법 및 예시 등) 1부(해당 경우에 한함) * 결합키 생성에 사용된 속성 제외 3. 결합 목적을 증명할 수 있는 서류 1부 4. 안전조치계획 및 이를 증빙할 수 있는 서류 1부

[개인정보처리자 결합신청기관 A사의 신청서 예시]

가명정보 결합 신청서

신청번호	A-2020-10-001

결합신청자			
기관명	해당없음	사업자등록번호 또는 법인등록번호	1975년 09월 19일
주소	서울시 서초구 서초대로 11길 ㅇㅇ	대표자명	해당없음
담당자	김결합	담당자 연락처 (전화, e-mail)	010-123-4567 abc@caaa.com
신청자 구분	[ ] 개인 [√] 공공기관 [ ] 비영리법인 [ ] 민간기관		

가명정보 제공		해당없음 [ ]
파일명	파일1	
제공방법	[√] 온라인 [ ] 오프라인	
제출예정일	2020 년 10 월 22 일	
전체 가명정보 제공 기관명(총수)	총 2개 : 홍길동(2019년도 종합), 결합신청기관 A사(파일명1) ※ 결합신청기관 B사는 별도의 가명정보를 제공하지 않고 활용만 함	
제공정보 요약	컬럼 수	30개
	전체 레코드 수	21,00개
	전체 파일 크기	46 MB

결합 결과물 이용	해당없음 [ ]
시계열 분석	[√] 해당없음 [ ] 시계열(신규) [ ] 시계열(추가, 결합접수번호 :)
결합목적	[√] 통계작성 [ ] 과학적 연구 [ ] 공익적 기록보존 등
세부결합목적	(구체적 목적 설명.... 통계작성 .....)

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

2020 년 10 월 22 일

신청인 김 결 합 (서명 또는 인)

결합전문기관의 장 귀하

첨부 서류
1. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류 1부 2. 결합 대상 가명정보에 관한 서류(전체 항목명 가명처리 대상 항목명, 가명처리 기법 및 예시 등) 1부(해당 경우에 한함) * 결합키 생성에 사용된 속성 제외 3. 결합 목적을 증명할 수 있는 서류 1부 4. 안전조치계획 및 이를 증빙할 수 있는 서류 1부

[개인정보처리자 결합신청기관 B사의 신청서 예시]

가명정보 결합 신청서

신청번호	A-2020-10-001

결합신청자			
기관명	해당없음	사업자등록번호 또는 법인등록번호	1978년 03월 05일
주소	서울시 서초구 효령로34길 ㅇㅇ	대표자명	해당없음
담당자	최가명	담당자 연락처 (전화, e-mail)	010-456-7890 abc@cbbb.com
신청자 구분	[ ] 개인 [ ] 공공기관 [ ] 비영리법인 [√] 민간기관		

가명정보 제공		해당없음 [√]
파일명		
제공방법	[ ] 온라인 [ ] 오프라인	
제출예정일	년 월 일	
전체 가명정보 제공 기관명(총수)		
제공정보 요약	컬럼 수	
	전체 레코드 수	
	전체 파일 크기	

결합 결과물 이용	해당없음 [ ]
시계열 분석	[√] 해당없음 [ ] 시계열(신규) [ ] 시계열(추가, 결합접수번호 :)
결합목적	[ ] 통계작성 [√] 과학적 연구 [ ] 공익적 기록보존 등
세부결합목적	(구체적 목적 설명.... 과학적 연구 .....)

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

2020 년 10 월 22 일

신청인 최 가 명 (서명 또는 인)

결합전문기관의 장 귀하

첨부 서류
1. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류 1부 2. 결합 대상 가명정보에 관한 서류(전체 항목명 가명처리 대상 항목명, 가명처리 기법 및 예시 등) 1부(해당 경우에 한함) * 결합키 생성에 사용된 속성 제외 3. 결합 목적을 증명할 수 있는 서류 1부 4. 안전조치계획 및 이를 증빙할 수 있는 서류 1부

[별지 9] 가명정보의 안전한 관리를 위한 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.

항목	내용
	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
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 수립·시행 2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치 3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 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

항목	내용
	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 ⑤ [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. ⑥ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다. ⑦ 개인정보보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상으로 점검·관리 하여야 한다.
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.

항목	내용
	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.

항목	내용
	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 일정 시간 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.
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 암호알고리즘

항목	내용
	으로 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	개인정보처리자는 개인정보 유출 등 개인정보 침해사고

항목	내용
(관리용 단말기의 안전조치)	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
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.