실무 표준 가이드라인

문서번호: PIPA-GUIDE-2026-01
개정일자: 2026년 7월
적용대상: 전사 데이터 활용 부서

개인정보 비식별화 및 가명처리 실무 매뉴얼

개인정보 보호법 준수를 위한 가명·익명처리 절차, 기법, 적정성 평가 및 안전 관리 표준

1. 개요 및 목적

1.1 작성 목적

본 매뉴얼은 기업 및 기관이 보유한 개인정보를 안전하게 활용하기 위해 「개인정보 보호법」 및 관계 법령에 의거하여 개인정보를 비식별화(가명처리 및 익명처리)하는 표준 절차, 기술적 처리 기법, 적정성 평가 기준 및 안전성 확보 방안을 제시합니다.

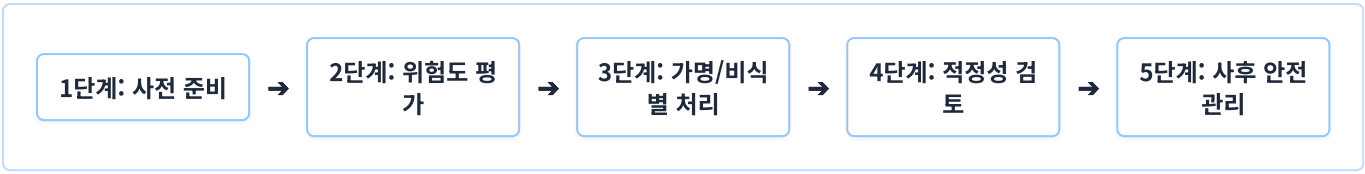
1.2 적용 범위

통계작성, 과학적 연구(상업적 목적 포함), 공익적 기록보존 등의 목적으로 개인정보를 가명처리하거나, 법적 적용 대상에서 완전 제외되는 익명정보로 전환하려는 모든 업무 절차에 적용됩니다.

1.3 핵심 용어 정의

구분	정의 및 핵심 특성	법적 적용 여부
가명정보 (Pseudonymized Data)	추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없도록 처리한 정보. 통계, 과학적 연구 목적 시 동의 없이 처리 가능.	개인정보 보호법 적용 대상 (안전성 확보조치 필수)
익명정보 (Anonymized Data)	합리적으로 고려할 수 있는 모든 수단을 사용하더라도 더 이상 특정 개인을 알아볼 수 없는 정보.	개인정보 보호법 적용 **제외**
식별자 (Identifier)	성명, 주민등록번호, 전화번호, 이메일 등 단독으로 특정 개인을 직접 알아볼 수 있는 정보.	삭제 또는 필수 대체 조치 대상
준식별자 (Quasi-Identifier)	연령, 성별, 거주지, 직업, 방문 기록 등 단독으로는 불분명하나 타 정보와 결합 시 개인 식별이 가능한 정보.	범주화, 마스킹 등 변형 조치 대상
추가 정보 (Additional Info)	가명정보와 결합하여 특정 개인을 알아볼 수 있게 하는 매핑 테이블, 해시 Salt, 암호화 키 등.	물리적·논리적 분리 보관 필수

2. 비식별화 표준 추진 절차 (5단계)



[1단계] 사전 준비
처리 목적(통계 작성, 과학적 연구 등) 법적 부합 여부 검토, 대상 데이터 항목 최소화 선별, 개인정보 처리 책임자 및 전담 인력 지정.

[2단계] 위험도 평가
데이터 자체 위험도(식별자 포함 여부, 준식별자 희소성) 및 처리 환경 위험도(내부망/외부망, 데이터 접근 권한 범위, 공개 데이터 결합 가능성) 평가.

[3단계] 가명처리 및 비식별 조치
식별자 완전 삭제 또는 해싱/대체키 변환. 준식별자에 대해 범주화, 마스킹, 노이즈 추가, 이상치 제거 등 목적에 적합한 비식별 기법 적용.

[4단계] 적정성 검토 및 심의
수학적 프라이버시 모델(k-익명성, l-다양성, t-근접성) 검증. 외부 전문가가 포함된 적정성 평가위원회를 구성하여 심의·승인 (부적합 시 재처리 또는 파기).

[5단계] 사후 관리 및 안전성 확보
추가 정보(결합키, Salt 등) 분리 보관, 가명정보 처리 대장 작성, 접근 권한 최소화 및 접속 기록 최소 3년 보관, 재식별 금지 모니터링.

3. 주요 비식별 조치 기법 및 실무 적용 예시

기법명	설명 및 처리 매커니즘	적용 전 (원본 데이터)	적용 후 (비식별 데이터)
삭제 (Deletion)	직접 식별자 또는 불필요한 속성 컬럼 전체를 완전 제거함	`주민번호: 920101-1234567`	(컬럼 완전히 삭제)
가명화/해싱 (Hashing)	식별자를 안전한 일방향 암호화 함수(SHA-256 + Salt)로 변환	`성명: 홍길동`	`e3b0c44298fc1c149...`
마스킹 (Masking)	식별 위험이 있는 일부 문자를 특수기호(`*`, `#`)로 대체	`전화번호: 010-1234-5678`	`010-****-5678`
범주화 (Aggregation)	구체적 수치나 상세 정보를 범주/구간/상위 개념으로 그룹화	`나이: 27세` `주소: 서울시 강남구 역삼동`	`나이: 20대 후반` `주소: 서울특별시 강남구`
라운딩 (Rounding)	수치 데이터를 올림, 버림, 반올림하여 대략적인 수치로 변환	`연봉: 45,320,000원`	`연봉: 45,000,000원`
노이즈 추가 (Noise Addition)	통계적 분포 특성을 유지하며 무작위 미세 변수값을 더하거나 뺌	`신장: 175.0cm`	`신장: 173.8cm`
레코드 삭제 (Row Deletion)	희소성이 높아 식별 가능성이 매우 높은 특이값(Outlier) 레코드 제거	`100세 이상 고령 환자 기록`	(해당 레코드 완전 삭제)

4. 수학적 프라이버시 보호 모델

4.1 k-익명성 (k-Anonymity)

연결 공격 방지

동일한 준식별자(Quasi-Identifier) 값의 조합을 가지는 레코드가 데이터집합 내에 **최소 k개 이상** 존재하도록 제한하는 모델입니다.

예시 ($k=3$): [30대, 남성, 서울 거주] 조합을 가진 데이터 레코드가 최소 3건 이상 존재해야 함.

4.2 l-다양성 (l-Diversity)

동질성/배경지식 공격 방지

k-익명성을 만족하더라도 민감한 정보(Sensitive Attribute)가 모두 동일할 경우 발생하는 동질성 공격을 방지하기 위해, 동일 동등류 내 민감 정보가 **최소 l개 이상의 서로 다른 유형**을 갖도록 제한합니다.

예시 ($l=3$): [30대, 남성, 서울] 집단 내 환자들의 진단 질병이 '위염', '당뇨', '고혈압' 등 최소 3가지 이상의 서로 다른 질환으로 구성되어야 함.

4.3 t-근접성 (t-Closeness)

쏠림/특이값 공격 방지

동일 동등류 내 민감 정보의 확률 분포와 전체 데이터 집합의 민감 정보 확률 분포 간의 거리가 **설정값 t 이하**가 되도록 유지하여 특정 민감 정보 편중을 방지합니다.

5. 법적 안전성 확보조치 준수사항

1. 추가 정보 분리 보관 및 관리

- 가명정보와 결합 키, 해시 Salt, 매핑 테이블 등 추가 정보는 물리적·논리적으로 분리 저장.
- 추가 정보에 접근 가능한 관리자를 최소한으로 제한 및 지정.

2. 기술적·관리적·물리적 보호조치

- **관리적:** 가명정보 처리 내부 관리계획 수립 및 정기 교육.
- **기술적:** 접근통제, 송수신 구간 암호화, 접속기록 월 1회 이상 점검.
- **물리적:** 전산실 및 자료보관실 출입 통제 및 잠금장치 설정.

3. 재식별 금지 및 사고 대응

- 특정 개인을 알아보기 위한 목적으로 가명정보를 처리하는 행위 엄금 (위반 시 형사처벌).
- 처리 중 특정 개인이 재식별된 경우 즉시 처리를 중단하고 지체 없이 회수·파기.

4. 처리 대장 작성 및 법정 보관

- 가명정보 처리 목적, 항목, 이용 내역, 제3자 제공 내역 기록.
- '가명정보 처리 대장'을 작성하여 **최소 3년 이상** 안전하게 보관.

6. [부록] 가명처리 및 비식별 적정성 평가 체크리스트

* 본 체크리스트는 적정성 평가위원회 심의 및 내부 결재용으로 활용할 수 있습니다.

구분	점 검 항 목	점검 결과	비고 / 조치 내용
사전준비	1. 법적 처리 목적(통계작성, 과학적 연구 등)에 정확히 부합하는가?	☐ 적합	
사전준비	2. 목적 달성에 필요한 최소한의 항목 및 데이터량만 선정하였는가?	☐ 적합	
위험도 평가	3. 직접 식별자와 준식별자 목록을 명확히 분류하고 식별 위험을 평가했는가?	☐ 적합	
위험도 평가	4. 활용 환경(내부 이용, 외부 제공, 데이터 결합 여부) 위험도를 검토하였는가?	☐ 적합	
비식별 처리	5. 직접 식별자는 전면 삭제하거나 일방향 해싱(Salt 적용) 등 안전하게 처리했는가?	☐ 적합	
비식별 처리	6. 특이값(Outlier), 희소 데이터를 보유한 레코드에 대해 적절히 조치하였는가?	☐ 적합	
적정성 검토	7. k-익명성 등 선택한 프라이버시 보호 모델 수준을 성공적으로 충족하는가?	☐ 적합	
적정성 검토	8. 외부 전문가가 포함된 적정성 평가위원회의 심의·승인을 완료하였는가?	☐ 적합	
안전관리	9. 추가 정보(매핑 테이블, 키, Salt 등)를 별도 물리/논리 공간에 분리 보관하는가?	☐ 적합	
안전관리	10. 가명정보 처리 대장을 작성하고 3년 보관 및 접근기록 모니터링 체계를 갖추었는가?	☐ 적합	

작성 및 검토자

부서/직급: _____

성 명: _____ (서명/인)

개인정보 보호책임자 (CPO) 승인

직 책: 개인정보 보호책임자

성 명: _____ (서명/인)

본 문서는 개인정보 보호법 및 KISA 가명정보 처리 가이드라인을 기초로 제작되었습니다.