

AI시대 비정형 데이터 가명정보 활용 방안

한국인터넷진흥원 강동우 수석 연구원

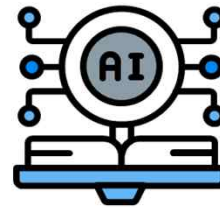
배경

: 데이터 수요
프라이버시 도전

▶ AI 대전환(AX)에 따른 이슈



데이터 활용 수요



AI 학습데이터 수집 경쟁



안전한 개인정보 처리



초거대 AI시대에서 데이터는 AI, 신기술 발전 등의 新산업 발전과
사회·경제적 혁신을 견인하는 핵심 원동력

배경

: 단계별 이슈

AI 단계별 주요 프라이버시 이슈

데이터 수집 단계

- 개인정보보호 원칙과 충돌
 - 방대한 데이터 처리를 기초로 하는 AI개발과 최소 수집원칙, 이용 목적 제한 등 개인정보 보호 원칙과 상충
- 학습 가능한 데이터 확보의 어려움

AI 학습 단계

- AI학습 과정에서 민감한 정보의 추론 가능성 발생
 - AI학습과정에서 공개된 정보 분석을 통해 공개되지 않은 정보를 추론
- 학습이 완료된 AI모델에 개인을 식별할 수 있는 정보가 포함될 위험

AI 서비스 단계

- 학습된 개인정보가 그대로 출력
- 개인식별 또는 민감정보 추론 목적으로 남용 우려



배경

: 도입



- ▶ AI 시대의 핵심 동력인 데이터를 개인정보를 침해하지 않으면서 활용할 수 있는 기반으로 개인정보보호법에 **‘가명정보 처리 특례’**를 도입
- ▶ 가명정보는 AI학습 등에 필요한 대규모 **개인정보를 동의 없이 활용**할 수 있는 **사실상 유일한 수단**
- ▶ 특히 텍스트·이미지·영상·음성 등 다양한 형태의 데이터를 **가명처리 하여 AI 학습데이터 활용 확대**



02

가명처리
절차

▶ 가명처리 절차



가명처리 절차

: 데이터 보유기관의
AI서비스 개발 시

▶ 데이터 보유기관이 가명처리 후 제공

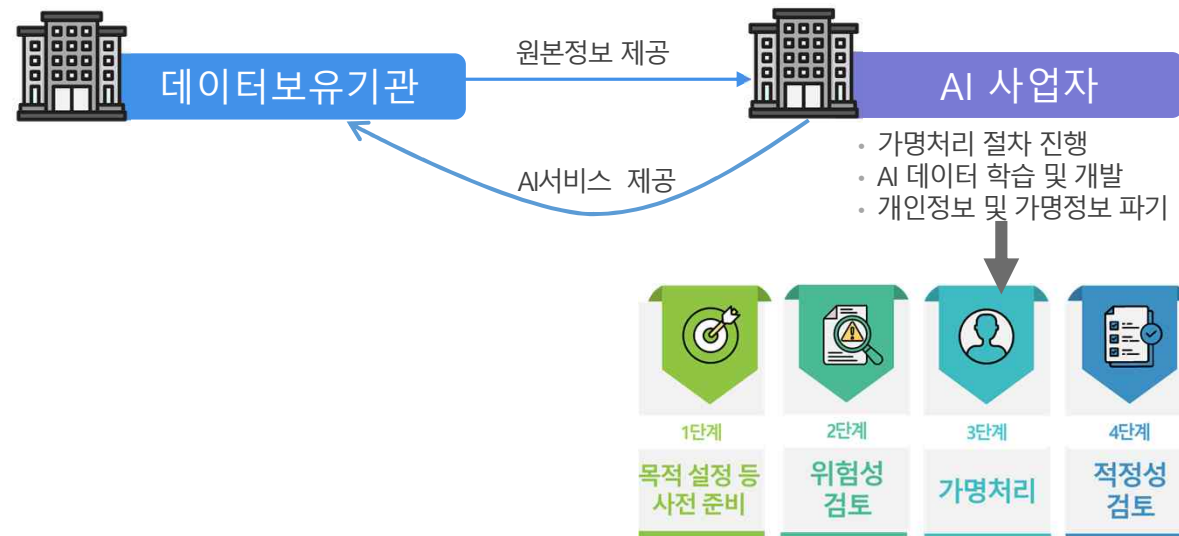


- 데이터보유기관과 AI 사업자는 가명정보를 활용을 위한 **가명정보 제공 계약 등** 체결
- 데이터보유기관의 **데이터 보유부서(담당자)**와 **AI 개발부서(담당자)**는 분리되어야 함

가명처리 절차

: 데이터 보유기관의
AI서비스 개발 시

▶ AI 사업자가 데이터 가명처리 후 AI개발



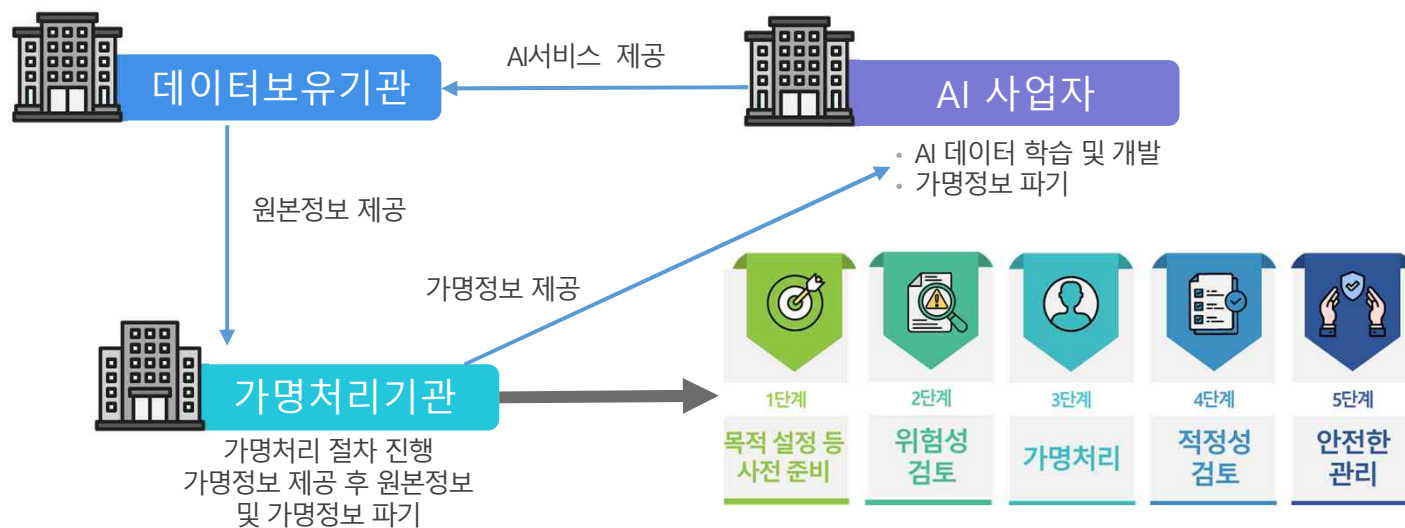
- 데이터보유기관과 AI 사업자는 **개인정보 처리 위·수탁 계약 체결**
- AI 사업자는 **데이터보유기관의 관리하에 원본정보를 가명처리 후 AI 데이터 학습**
- AI 사업자의 **가명처리 부서(담당자)**와 **AI 데이터 학습 및 개발 부서(담당자)**는 **분리**되어야 함

02

가명처리 절차

: 데이터 보유기관의 AI서비스 개발 시

▶ 제3의 가명처리 기관이 가명처리 후 AI개발



- 데이터보유기관과 가명처리기관은 가명처리를 위한 **개인정보 처리 위·수탁 계약 체결**
- 가명처리기관은 **데이터보유기관의 관리하에** 원본정보를 가명처리 후 AI개발 기업에 **가명정보 제공**
- 데이터보유기관의 **데이터보유부서(담당자)**와 **AI개발부서(담당자)**는 **분리**되어야 함

03

개인정보 이노베이션 존

: 개념

▶ 개인정보 이노베이션 존

연구자스타트업들이 **개인정보(특히, 가명정보)**를 보다 **유연하고 탄력적으로 활용**할 수 있는 공간

AI, 비정형데이터 활용 요구에 따라 데이터 처리의 **환경적 안전성**을 **높임**으로써,
개인·가명정보를 보다 **유연하게 활용**할 수 있는 제도 마련

▶ 개인정보 이노베이션 존 주요 기능

가명정보의 유연한 활용	가명정보의 장기활용 및 재사용	PET 실증
<ul style="list-style-type: none"> · 데이터품질 훼손 최소화를 위해 가명처리 수준의 적정수준으로 완화 · 결합률 극대화를 위해 CI(Connecting Information) 일부값 등 다양한 결합키 사용 허용 · 비정형(영상, 이미지, 텍스트 등) 빅데이터 가명 처리 시, 샘플링 검사 허용 	<ul style="list-style-type: none"> · AI개발 등 지속적 반복적 연구목적의 경우, 가명정보장기간보관 가능 (안심구역 내 보관·활용, 추가 연장신청도 가능) · 개인정보안심구역에 보관된 가명정보는 제3자가 재사용신청하여 활용 가능 (원 보유기관과 협의 지원) 	<p>PET 기술은 기존 제도 적용이 모호하거나 안전성 검증체계가 없어서 활용 부진</p> <p>전문심의위원회의 심의·검증하에 PET를 적용한 개인정보 처리 폭넓게 허용</p> <p>PET(Privacy Enhancing Technology) :가명·익명처리기술,동형암호,합성데이터,차분 프라이버시 등 프라이버시를 향상시킬수 있는 다양한 개인정보보호 활용기술</p>



03

개인정보 이노베이션 존

: 현황

▶ 개인정보 이노베이션 존 지정 현황

운영 기관 지정('23.12월)



'24.3월 개소(대전)



'24.7월 개소(고양)

운영 기관 지정('24.6월)



'25.3월 개소(김천)

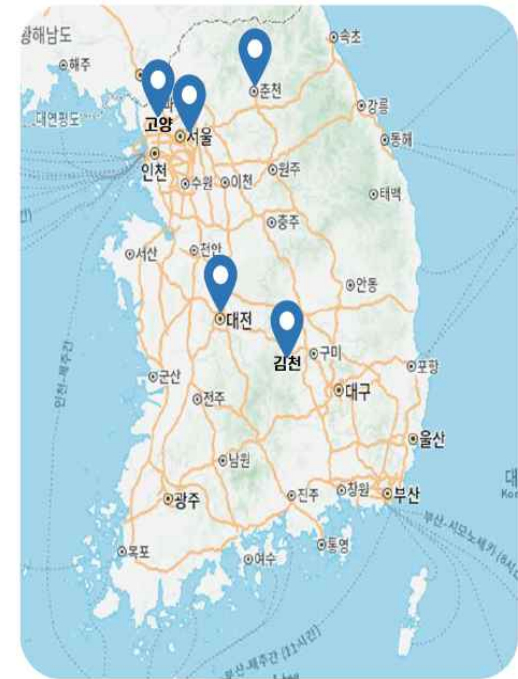


'24.12월 개소(서울)



'25.1월 개소(춘천)

기관명	특화분야	위치	연락처
통계청	국가통계	대전광역시 서구 한밭대로 713, 통계데이터센터 13층	044-481-2380
국립암센터	보건의료	경기도 고양시 일산동구 일산로 323, 연구동 7층(국가암데이터센터)	031-920-0770
한국도로공사	국가교통	경상북도 김천시 혁신8로 77, 본관 3층	031-5179-6134
한국사회보장정보원	사회복지	서울특별시 광진구 능동로 400, 보건복지행정타운 14층	02-6360-4685
더존비즈온	정밀의료	강원특별자치도 춘천시 남산면 버들길 130, 더존ICT그룹 강촌캠퍼스 별관 4층	02-6233-0640



비정형 데이터

: 가이드라인 개정

▶ 비정형데이터 가명처리 기준 마련

AI 기술 발전과 컴퓨팅 자원 발달로 데이터 활용 수요가 전통적 정형데이터(수치)에서 비정형데이터(이미지, 영상, 음성, 텍스트)로 변화

* 전 세계 데이터 중 이미지, 영상, 음성, 텍스트 등 비정형데이터가 최대 90%를 차지(IDC, '23)

참고 * 비정형데이터 : 정의된 구조가 없이 정형화되지 않은 데이터(이미지·영상, 텍스트, 음성 등)로, AI 연구가 급증하고 비정형 데이터 자체로 학습이 가능해지자, 활용 수요가 크게 증가

이에 자율주행차, CCTV, IoT 등에서 수집된
비정형데이터(영상, 음성, 텍스트 등)의 가명처리 기준 마련
따른 「**가명정보 처리 가이드라인**」 개정안 발간(24.2.)



04

비정형 데이터

: 기본원칙

● ● ● ● ● 11

▶ 비정형데이터 가명처리 기본 원칙

01

데이터 처리 목적, 환경, 민감도 등을 종합적으로 고려하여 개인식별 위험성이 있는 정보를 판단하고, 합리적인 처리 방법, 수준 설정

02

가명처리 기술의 한계 등을 보완하기 위해 사전 준비단계(연구 및 기술 개발 기획)부터 위험성을 충실히 검토하고 적절한 안전조치를 수행

03

데이터 복원기술 발달 등에 대응하여, 가명 처리된 비정형데이터 활용 시 관련 시스템·SW의 접근·사용 제한 등 통제방안 마련



비정형 데이터

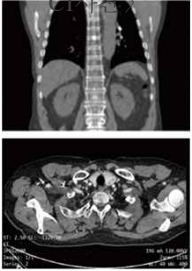
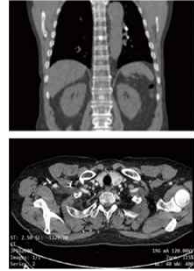
: 시나리오

▶ 주요 비정형데이터 가명처리 시나리오

(사례1) 유방암·골밀도 감소 여부 진단 AI 개발

대학병원이 보유한 유방암 환자 CT사진(영상:이미지) 및 병리기록지(텍스트)를 가명처리하여 유방암 및 골밀도 감소 여부 진단 AI 개발을 위한 내부 연구에 활용한 사례

개인식별 위험이 발생하지 않도록 처리환경을 안전하게 통제하고 복원 SW 반입 제한 조치 등을 통해 별도의 가명처리 없이 CT 사진을 그대로 활용

 <p>〈흉부 CT사진〉</p>	<p>개인식별 위험성 검토</p>	<ul style="list-style-type: none"> • 흉부 CT사진만으로는 개인식별 위험성 거의 없음 • 개인당 200장씩 촬영된 CT사진이 활용되는 연구로서 3차원 재건 기술 등을 통해 신체 형상의 입체적 복원이 가능하고, 복원 시 특이한 외형·흉터 등이 있는 극히 일부 환자의 경우 낮은 확률로 개인식별 위험성 존재 • 클라우드 기반 폐쇄연구분석환경*을 이용 하고 인가되지 않은 데이터·프로그램 반입을 철저히 통제하고 있어 3차원 재건기술 적용 불가 *클라우드 서버에 데이터를 저장하고 타 외부망에서는 클라우드 서버 접속이 제한되는 분석실에서 인가 받은 인원만 데이터 접근 가능 	<p>(그대로 활용)</p> 
	<p>데이터 처리 방안</p>	<p>⇒ 3차원 재건으로 인한 개인식별 위험성이 존재하나, 환경적 통제로 인해 해당 위험의 발생 가능성이 없으므로 별도의 가명처리 없이 그대로 활용 가능</p>	





▶ 주요 비정형데이터 가명처리 시나리오

(사례2) 구강질환 진단 AI 개발

대학병원이 보유한 구강 건강검진 촬영 사진(이미지)을 가명처리한 뒤 기업에 제공하여, 충치·치주염 등 구강질환을 진단하는 AI 연구개발에 활용한 사례

연구 목적에 필요 없는 영역을 블러링 처리하고, 메타데이터를 삭제하여 활용

<p>< 구강 촬영사진 ></p> 	<p>개인식별 위험성 검토</p> <ul style="list-style-type: none"> 구강사진 자체로는 개인식별 위험성 거의 없음 충치 영역 외 부분은 연구에 필요 없음 구강사진에 대한 메타데이터(이름, 나이 등)는 구강사진과 결합되어 개인식별 위험성 존재 	<p>(충치 부분: 그대로 활용) (그 외: 블러링 처리)</p> 
	<p>데이터 처리 방안</p> <p>⇒ 연구에 필요한 충치 영역은 그대로 활용하고, 연구에 필요 없는 그 외 영역은 블러링 처리</p> <p>※ 블러링 수준은 현재 복원기술 발전수준 및 데이터 처리 환경 (타정보·복원기술 접근성) 등을 고려하여 설정</p> <p>⇒ 메타데이터는 연구에 필요 없어 삭제</p>	



비정형 데이터


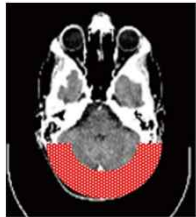
: 시나리오

▶ 주요 비정형데이터 가명처리 시나리오

(사례3) 안면골 골절 진단 AI 개발

대학병원이 보유한 Facial CT 사진을 가명처리하여, 안면골(얼굴뼈) 골절여부를 진단하는 AI 개발을 위한 공동연구를 대학병원과 민간기업이 함께 수행한 사례

개인식별 위험성을 낮추기 위해 연구목적에 필요 없는 영역만 마스킹 처리하여 활용

<p>< Facial CT사진 ></p> 	<p>개인식별 위험성 검토</p>	<ul style="list-style-type: none"> • CT사진 자체로는 개인식별 위험성 거의 없음 • 3차원 재건 기술을 통해 입체적 복원이 가능하며, 복원 시 특이한 얼굴·외형, 알려진 얼굴 등 극히 일부 환자의 경우 낮은 확률로 개인식별 위험성 존재 • 대용량 영상·이미지를 활용하는 연구로 3차원 재건이 가능하나, 가장자리 마스킹 기법을 활용하여 3차원 재건 공격 위험을 낮출 수 있음 • 후두부(뇌 뒷부분) 영역은 연구에 필요 없음 	<p>(안면부 : 그대로 활용) (후두부 : 마스킹 처리)</p>
	<p>데이터 처리 방안</p>	<p>⇒ 연구에 필요한 안면부는 그대로 활용하고, 연구에 필요없는 후두부는 마스킹하여 3차원 재건위험을 낮추고 활용</p>	



비정형 데이터

: 시나리오



▶ 주요 비정형데이터 가명처리 시나리오

(사례4) 자율주행차 주행 시 비정상 상황인지 AI 개발

연구기관이 보유한 도로 주행상황 촬영 영상을 가명처리한 뒤 기업에 제공하여, 자율주행자동차 운행 시 비정상 상황*을 인지하는 AI 연구개발에 활용한 사례

* 사람이 차도에 뛰어드는 상황, 다른 차가 갑자기 앞에 끼어드는 상황, 무단횡단 등

연구 목적에 필요 없는 영역만 마스킹 처리하여 활용

<p>〈 얼굴·차량번호판 〉</p> 	<p>개인식별 위험성 검토</p>	<ul style="list-style-type: none"> • 사람의 얼굴이 선명히 보이는 경우, 차량 번호판이 그대로 노출되어 차량 탑승자 유추가 가능한 경우 등에 개인식별 위험성 존재 • 연구목적상 사람·차량의 전체 형상과 움직임만 파악 가능하면 되므로, 얼굴·차량번호판은 마스킹해도 무방 	<p>(마스킹 처리)</p> 
	<p>데이터 처리 방안</p>	<p>⇒ 얼굴·차량번호판 영역을 사람과 컴퓨터가 식별 불가능한 수준으로 마스킹하여 활용</p>	



비정형 데이터





: 시나리오

▶ 주요 비정형데이터 가명처리 시나리오

(사례5) 고속도로 다인승전용차로 단속 AI 개발

지자체가 CCTV로 촬영한 고속도로 통행차량 이미지를 가명처리한 뒤 기업에 제공하여,
다인승 전용차로 위반*을 단속하는 AI 개발에 활용한 사례
* 3명 이상 승차하지 않은 승용·승합자동차가 다인승전용차로를 이용한 경우

연구 목적에 필요 없는 영역만 블러링 처리하여 활용

<p>〈도로 통행차량 사진〉</p> 	<p>개인식별 위험성 검토</p>	<ul style="list-style-type: none"> · 탑승자의 얼굴이 선명하게 촬영된 경우, 차량 외부에 특이점이 있는 경우 등은 개인식별 위험성 존재 · 연구 목적상 특정인 식별·구분이 필요없고 (1)사람인지 아닌지 여부, (2) 차량 탑승인원이 몇 명인지만 확인할 수 있으면 됨 · AI가 사람인지 여부는 판단할 수 있도록 하되, 탑승자가 누구인지는 판별 불가능 하도록 블러링 등 처리 필요 	<p>(① 탑승자 위치·범위 파악)</p> 
<p>〈특이점 있는 차량〉</p> 		<p>⇒ 이점이 있는 차량 이미지는 삭제 ⇒ 블러링 수준(1~10단계)별로 데이터를 가명처리한 후, 식별위험이 없으면서 AI 정밀도를 어느 정도 확보할 수 있는 블러링 수준 결정 ※ 블러링 수준은 현재 복원기술 발전수준 및 데이터 처리 환경 (타 정보·복원기술 접근성) 등을 고려하여 설정</p>	<p>(② 블러링 처리)</p> 



비정형 데이터


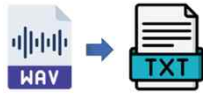

: 시나리오

▶ 주요 비정형데이터 가명처리 시나리오

(사례6) 음성데이터 활용 시 기반 보이스피싱 범죄 예방

보이스피싱 범죄 상황 음성데이터를 가명처리하여 가명정보로 학습한 AI 기술 활용하여 보이스 피싱 탐지·예방

음성정보를 텍스트로 변환(STT, Speech To Text)한 뒤 가명처리 후 AI 모델 학습에 활용

<p>〈음성 상담파일〉</p>  <p>목소리 개인식별정보</p>	<p>개인식별 위험성 검토</p> <ul style="list-style-type: none"> • 보이스피싱 음성파일에는 개인의 실제 음성데이터(목소리, 음색, 억양, 발음 등)가 포함되어 있고, 대화 내용에는 다양한 개인식별가능정보가 정제되지 않은 형태로 존재 • 실시간 보이스피싱 탐지 AI 모델 개발에는 개인 질의-응답과 통화내용(대화 문맥 등)의 흐름 파악이 중요하며 실제 음성 자체는 필요하지 않음 	<p>(① 텍스트로 변환)</p> 
	<p>데이터 처리 방안</p> <p>⇒ 음성변환(STT) 기술을 통해 텍스트로 변환한 뒤, 개인식별 위험성이 있는 항목들을 가명처리(치환·삭제)하여 활용</p> <p>⇒ 텍스트 데이터에 대한 가명처리 기술의 정확도가 100%가 아니므로, 추가 전수 검사를 통해 식별 위험성이 있는 정보를 제거</p>	<p>(② 개인식별정보 치환삭제)</p> 



05

정부 지원 사항

● ● ● ● ● 18



감사합니다

THANK YOU

문의처 : 서울 가명정보 활용지원센터
02-431-4835

help@dataprivacy.go.kr

누리집 : [가명정보.한국\(dataprivacy.go.kr\)](http://가명정보.한국(dataprivacy.go.kr))

