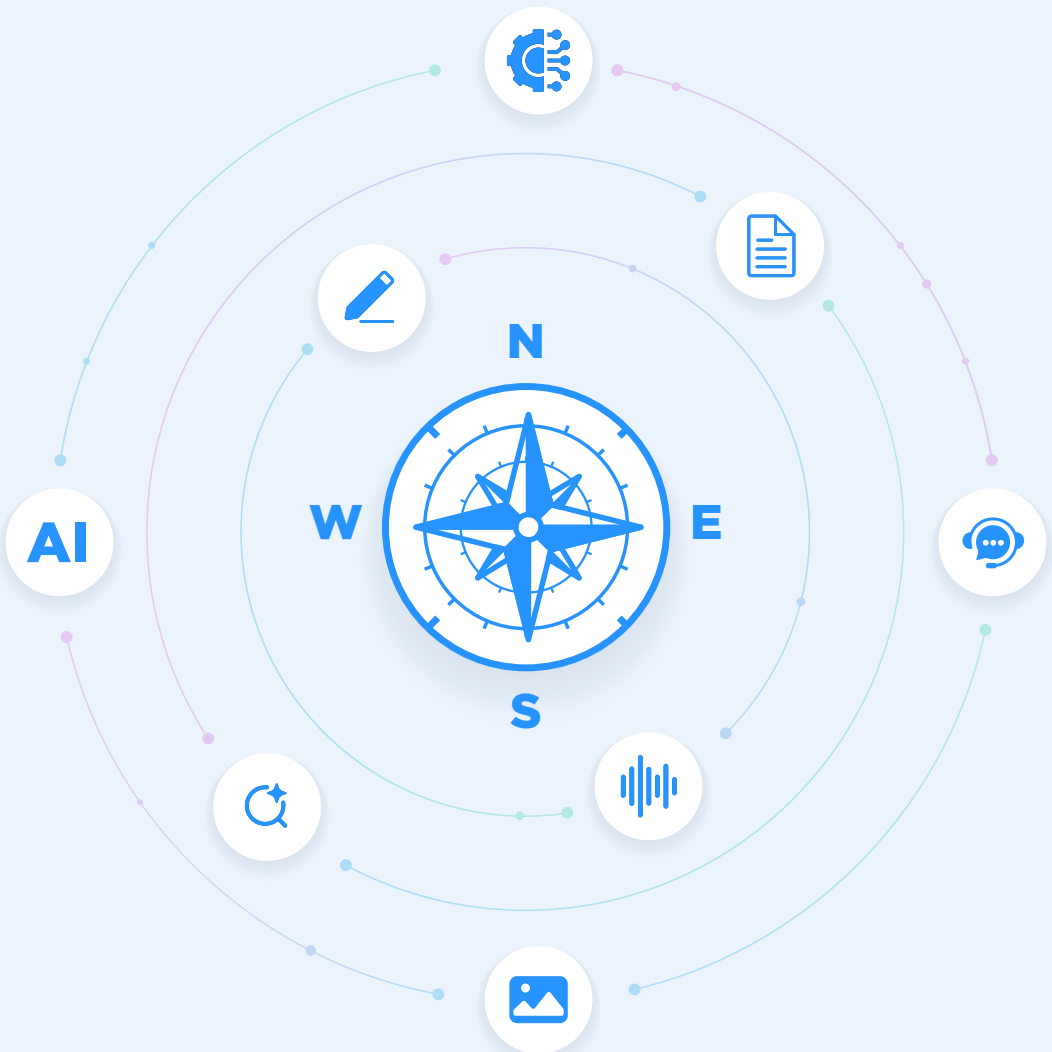
생성형 AI 서비스 이용자를 위한 개인정보 보호 가이드



개인정보보호위원회

I 들어가며

1. 발간 배경 및 목적

생성형 AI는 일상과 업무 전반에서 자연스럽게 활용되는 도구로 자리잡았습니다. 문서 작성, 정보 탐색, 대화와 상담에 이르기까지 다양한 상황에서 AI의 도움을 받는 일이 일반화되고 있습니다.

이처럼 생성형 AI 활용이 늘어나면서 이용자들은 자신이 입력한 정보가 어떻게 쓰이는지, 삭제한 내용은 어떻게 처리되는지, 이 과정에서 개인정보는 어떻게 보호되는지 궁금해하고 있습니다.

본 가이드는 이용자들의 이러한 궁금증에서 출발하여 생성형 AI 환경에서 개인정보가 어떻게 처리되는지를 쉽게 이해할 수 있도록 돕고, 자신의 정보를 안전하고 현명하게 관리할 수 있는 방법을 안내하고자 합니다.

그동안 관련 안내가 주로 사업자를 대상으로 이루어졌다면, 이번 가이드는 이용자 관점에서 복잡한 법률 용어나 기술 설명은 최대한 덜어내고, 일상에서 생성형 AI를 이용하며 직접 점검하고 실천할 수 있는 방안 중심으로 정리하였습니다.

2. 누구를 위한 자료인가

본 가이드는 생성형 AI를 활용하는 모든 이용자를 위한 자료입니다. 업무에 활용하는 직장인, 학습 목적으로 이용하는 학생, 일상에서 다양한 서비스를 접하는 일반 시민까지, 연령과 직업에 관계없이 누구나 쉽게 참고할 수 있도록 마련하였습니다.

생성형 AI를 자주 사용하는 분이라면 자신의 개인정보가 어떻게 처리되는지 점검하는 데, 처음 접하는 분이라면 안전하게 시작하는 데 도움이 될 것입니다.

3. 어떻게 구성되었는가

본 가이드는 실제 민원 사례와 언론 보도, 해외 정책 동향 등을 참고하여 마련하였습니다.

먼저 II 장에서는 생성형 AI 서비스 이용 과정에서 개인정보가 처리되는 주요 지점을 한눈에 보여주는 생애주기 도식을 제시하고, III장에서는 이용자가 자주 궁금해하는 질문을 선별해 질문과 답변(Q&A) 형식으로 정리하였습니다.

처음부터 차례로 읽으며 전반적인 내용을 익힐 수도 있고, 필요한 질문만 선택해 찾아보는 방식으로도 활용할 수 있습니다. 생애주기 도식에는 각 단계별로 관련 Q&A 번호가 표시되어 있어, 궁금한 시점부터 바로 찾아볼 수 있습니다.

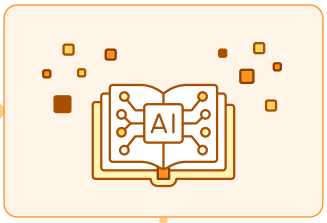
생성형 AI란?

이용자의 질문이나 요청에 따라 글, 이미지, 음성 등 새로운 결과물을 만들어내는 인공지능 기술을 말합니다. 대표적인 서비스로 ChatGPT, Claude, Gemini 등이 있으며, 문서 작성·정보 탐색·번역·이미지 생성 등 다양한 용도로 활용되고 있습니다. 최근에는 이용자를 대신해 일정·메일·검색 등 여러 작업을 수행하는 에이전틱 AI 형태로도 발전하고 있습니다.

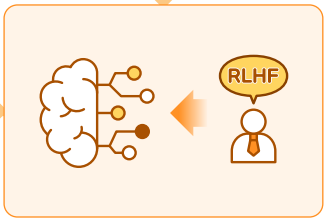
Ⅱ 생성형 AI 서비스 이용 관련 개인정보 처리 생애주기
: 데이터 수집부터 외부 서비스 연동까지

다음 그림은 생성형 AI 서비스를 이용하는 과정에서 개인정보가 처리될 수 있는 주요 지점을 한눈에 보여줍니다. 각 단계별 유의사항은 박스에 표시된 관련 Q&A 번호를 따라가면 자세히 확인할 수 있습니다.

데이터 수집
AI 개발 개선을 위해
다양한 데이터가 수집될 수 있어요



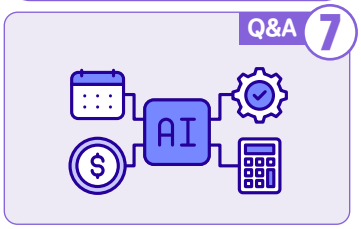
사전 학습 (Pre-training)
AI 학습 과정에서 개인정보가
포함된 자료가 활용될 수 있어요



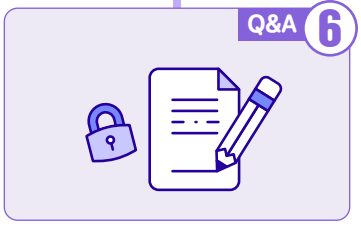
사후 학습(Post-training)
사전 학습된 모델을 특정 분야에 특화시키거나
답변 품질을 높이기 위해 추가 학습하는
과정에서 내 개인정보가 활용될 수 있어요

안전장치
AI가 개인정보를 암기하거나
말하지 않도록 안전 장치를 둬요.
(그래도 애초에 입력하지 않도록 주의하세요)

서비스 이용 환경



외부 서비스 연동(에이전틱 AI 포함)
메일, 일정, 결제 등 다른 서비스와 연결해 대신 작업을 수행해줘요.
내 개인정보가 외부 서비스로 어떻게 전달되는지 확인해야 해요.



답변에 개인정보 포함된 경우 신고•문의하기

실시간 상호작용 또는 외부 지식 참조
질문에 대답하기 위해 외부의 정보를 참고해요.
이 때 내가 입력한 개인정보와 나와 한 대화를
AI가 배우고 말하게 될 수 있어요.

학습 활용 여부 확인(옵트 아웃)
내가 입력한 내용이 AI 학습에
활용될 수 있어요. 원치 않는다면
'학습 거부'로 설정하세요.

대화기록 저장• 삭제 설정
대화를 삭제해도 보안 등을 위해
일정기간 보관할 수 있어요.

국외이전 가능성 확인
글로벌 AI 서비스를 이용하면
국내에서 사용하더라도 데이터가
국외로 이전될 수 있어요

III 주요 Q&A

다음은 생성형 AI 서비스 이용 과정에서 이용자들이 자주 마주하는 질문 8가지를 선별하여 정리한 것입니다. 각 질문에 대한 답변과 이용자가 직접 점검하고 실천할 수 있는"똑똑한 관리법"을 제시하였습니다.

01
AI에 입력한 내용들이 학습을 위해서도 사용되나요?

- **서비스마다 다르며, 같은 서비스라도 설정에 따라 달라질 수 있습니다.** 일부 서비스는 이용자가 입력한 질문, 파일, 이미지, 음성 등을 AI 모델 개선을 위해 학습에 활용할 수 있습니다.

- 반면, 답변 제공 등 서비스 운영상 필요한 범위 내에서만 처리하고 학습에는 활용하지 않을 수도 있습니다. 최근에는 대화 기록을 남기지 않거나 학습에 활용하지 않는 임시 대화 기능을 제공하는 서비스[1]도 늘어나고 있습니다.

- 따라서 이용 전에는 **입력 내용이 기본적으로 학습에 활용되는지, 이용자가 이를 직접 설정할 수 있는지 서비스별 정책을 확인**하는 것이 바람직합니다.

서비스별 정책 확인 시 살펴볼 점

> ·**처리 목적** : '서비스 제공' 외에 품질 개선, 학습, 모니터링 등 목적이 있는지
> ·**처리 범위** : 대화 내용, 업로드 파일, 접속·사용 기록 등 무엇을 수집·이용하는지
> ·**데이터 설정** : 학습 활용 배제, 기록 저장 끄기, 삭제 요청 절차 등이 있는지

[1] 예: ChatGPT – Temporary Chat / Google Gemini – Temporary Chat / xAI Grok – Private Chat 등

이용자를 위한 똑똑한 관리법

01

서비스 이용 전 입력 데이터의
학습 활용 여부를 확인하고,
원하지 않는 경우 **제한 설정**하기

02

주민등록번호, 여권번호, 계좌번호,
비밀번호, 인증코드 등 **중요한 정보는**
아예 입력하지 않기

데이터 학습 활용 배제(opt-out) 방법 예시

설정 → 데이터 제어/프라이버시 → 채팅 기록 및 학습 OFF

설정 → 활동제어 → OFF

02

AI 서비스 내 대화 기록을 삭제하면 완전히 지워지나요?

대화 기록을 삭제하더라도, AI 시스템 전반에서 해당 내용이 한 번에 즉시 완전히 제거되기보다는 **서비스 운영 방식에 따라 여러 단계에 걸쳐 관리·삭제될 수 있습니다.**

이용자가 '삭제' 버튼을 눌렀을 때의 일반적인 처리 흐름은 다음과 같습니다.

> **① 이용자 화면에서의 삭제(접근 차단)**
> 삭제된 대화는 계정의 대화 목록에서 더 이상 조회되지 않으며, 이용자는 해당 내용을 다시 확인하거나 이어서 활용할 수 없게 됩니다. 일반적으로 이용자가 인식하는 '삭제'는 이 단계에 해당합니다.
>
> **② 서비스 운영을 위한 보관(일정기간 유지)**
> 다만 서비스의 안정적 운영, 보안 대응, 오류 점검, 법적 의무 이행 등을 위해 해당 데이터가 일정 기간 서버 또는 백업 시스템에 보관될 수 있습니다.
>
> 이 경우, 보관 기간과 접근 범위는 서비스별 정책에 따라 달라질 수 있습니다.
>
> **③ 모델 개선이나 품질 향상 목적과의 관계**
> 삭제 이전에 입력된 내용이 서비스 정책에 따라 모델 개선·품질 향상 목적에 활용되었거나 통계 처리 또는 비식별 형태로 별도 관리되고 있을 가능성도 있습니다.

따라서 이용자는 '삭제' 기능의 의미와 한계를 이해하고, **데이터의 보관 여부, 활용 범위 (학습 포함), 보관 기간 및 관련 설정을 개인정보처리방침, 이용약관 또는 서비스 설정을 통해 확인**할 필요가 있습니다.

아울러, 민감한 정보의 경우에는 사후 삭제에만 의존하기보다 **처음부터 입력을 최소화하는 것이 보다 안전합니다.** 또한, 미성년자가 이용하는 경우 **보호자와 함께 서비스의 대화 기록 저장·삭제 설정을 확인**하는 것이 바람직합니다.

이용자를 위한 똑똑한 관리법

01

서비스의
'대화 기록 삭제' 기능과
'데이터 보관 정책' 확인하기

02

기록 기능(저장/히스토리)이
있다면 **기본값 점검**하고
필요시 끄기

03

기기(브라우저)에도
다운로드한 파일 등이 남을 수
있으니, **로그아웃 후
파일도 완전히 삭제**하기

03

AI 서비스 이용 과정에서 개인정보가 해외에 전송될 수도 있나요?

- **가능합니다.** 국내에서 서비스를 이용하더라도 데이터를 저장하거나 처리하는 서버가 해외에 있으면 입력한 대화 내용, 업로드 파일, 접속 기록 등이 해외로 전송되어 보관·처리될 수 있습니다.

- 특히 글로벌 AI 서비스는 여러 나라의 데이터센터를 함께 이용하거나, 장애 대응, 보안 점검, 고객 지원 등을 위해 해외 법인이 데이터에 접근하는 경우도 있습니다.

- 내 정보가 어느나라에서 관리되는지 궁금하거나 중요한 자료를 입력하려는 경우에는 **개인정보처리방침이나 전자우편 등을 통해 국외이전 여부, 이전 항목, 이전 국가 등을 확인 후 입력**하는 것이 바람직합니다.

이용자를 위한 똑똑한 관리법

01

개인정보처리방침 등을 통해
'국외 이전', '해외 이전'
관련 항목 찾기

02

이전 국가, 이전 항목,
이전 목적, 보유기간,
이전받는 자 정보를 살펴보기

03

민감한 자료는
국외 이전 여부를 확인한 후
입력 여부 결정하기

04

AI 챗봇에 입력한 대화 내용도 개인정보가 될 수 있나요?

가능합니다. AI 챗봇에 입력하는 문장은 일상 대화처럼 보일 수 있지만, 개인을 알아볼 수 있는 단서가 포함되어 있다면 개인정보에 해당할 수 있습니다.

예를 들어, 이름·연락처·주소·계좌번호처럼 특정 개인을 직접 식별할 수 있는 정보뿐만 아니라, "○○초 3학년 2반 담임", "지난주 수요일 ○○병원 진료결과"처럼 **여러 단서가 결합되어 특정 개인이 쉽게 드러날 수 있는 정보도 개인정보**로 볼 수 있습니다.

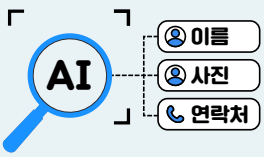
아울러, **AI 서비스는 이용 과정에서 텍스트뿐 아니라 이미지나 음성 업로드를 통해서도 대화와 단서가 계속 축적**됩니다. 한 번의 입력으로는 식별이 어려워 보여도, 이처럼 **누적된 정보들이 결합**되면 **특정 개인이 식별**될 수 있으므로 주의해야 합니다.

따라서 이용자는 AI 서비스를 이용하기 전 **입력하려는 내용에 개인을 식별할 수 있는 정보가 포함되어 있는지 확인할 필요**가 있습니다. 특히 가족, 동료 등 **제3자에 관한 정보를 입력할 때에는 본인뿐 아니라 타인의 개인정보까지 함께 처리될 수 있다는 점에 유의**해야 합니다.

이용자를 위한 똑똑한 관리법

01

입력 전, 내용에 **개인을 식별할 수 있는 정보가 포함되어 있는지 확인**하기

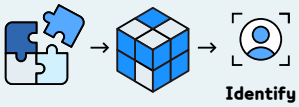


02

본인뿐 아니라 가족·동료 등 **제3자의 정보가 포함되어 있는지 점검**하기

03

한 번의 대화에서 안전해 보이더라도, **누적되면 식별로 이어질 수 있음**을 유념하기



05

업무 관련 자료나 조직 내부 정보를 AI 서비스에 입력해도 되나요?

- 업무 자료나 조직 내부 정보를 AI 서비스에 입력할 수 있는지는 **해당 정보의 성격, 소속 조직의 정책 그리고 이용하는 AI 서비스의 데이터 처리 방식에 따라 달라**집니다.

- 우선, 소속 조직에 **AI 서비스 이용과 관련한 내부 지침이 있거나 별도로 승인된 도구가 있는지 확인**하는 것이 중요합니다. 일부 조직은 보안이나 개인정보 보호를 이유로 특정 서비스만 허용하거나, 입력 가능한 정보의 범위를 제한하고 있을 수 있습니다.

- 특히, 조직 내부 정보에는 개인정보뿐 아니라 미공개 업무 정보, 내부 의사결정 내용, 계약 관련 정보 등이 포함될 수 있으므로, 단순히 개인정보가 아니라는 이유만으로 자유롭게 입력해서는 안 됩니다.

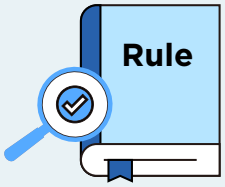
- 아울러, **고객·거래처 정보, 인사 정보 등 제3자의 개인정보가 포함된 자료**를 입력할 때는 **사전 동의나 법적 근거 없이 외부로 전달될 위험**이 있다는 점에 특히 유의해야 합니다.

한편, 업무 목적으로 AI 서비스를 사용할 때는 입력한 내용이 모델 학습이나 다른 목적으로 활용되지 않도록 계약·정책상 통제되는 기업용 라이선스 사용을 고려하는 것이 바람직합니다.

이용자를 위한 똑똑한 관리법

01

소속 조직의 AI 서비스 이용 지침을 확인하기

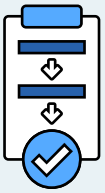


02

조직 내부 승인된 도구 활용하기:
승인된 계정/도메인/환경인지 확인하기

03

(필요 시)
반출 승인 절차 준수하기



06

AI 답변에 나와 가족 등 개인정보가 포함되어 있으면 어떻게 해야 하나요?

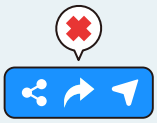
- 본인 또는 가족 등 제3자의 개인정보가 포함된 답변이 생성된 경우 **해당 내용을 추가로 공유하거나 활용하지 않는 것이 우선입니다.**
- 이러한 정보 생성은 과거 대화 내용이 반영되었거나, 계정을 타인과 함께 사용했거나, 공용 기기 또는 공용 장소에서 사용한 기록이 남아있는 경우 등 다양한 원인으로 발생할 수 있습니다. 따라서 **계정 이용 이력, 최근 대화 내역, 로그인 상태 등을 함께 점검해 볼 필요가 있습니다.**
- 다음으로, 이용 중인 서비스에서 제공하는 **신고 또는 피드백 기능을 활용하여 해당 답변에 개인정보가 포함되어 있음을 알리고, 삭제 등 필요한 조치를 요청**할 수 있습니다. 신고 시에는 가능한 한 화면 캡처 등 증빙을 함께 제출하면 처리에 도움이 됩니다.
- 만약, 미성년 자녀의 개인정보가 포함된 경우에는 부모 등 법정대리인이 아동의 권리 보호를 위해 보다 신속하게 삭제 요청을 진행할 필요가 있습니다.
- 아울러, 유사한 정보가 다시 생성되지 않도록 과거 입력 내용을 점검하고 관련 대화 이력을 삭제하는 한편, 데이터 저장·활용 및 외부 연동과 관련된 설정도 함께 확인·조정하는 것이 바람직합니다.

이용자를 위한 똑똑한 관리법

01

공유중단

답변 결과를
전송/게시하지 않기



02

증빙확보

신고를 위한
화면 캡처하기

03

기록삭제

해당 대화/파일/생성물을
서비스 내에서 삭제하기

04

연동해제

드라이브·메일 등 필요 없는
외부 연동이 있다면 권한 회수

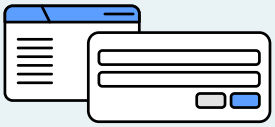
05

사업자신고

서비스 내 신고/문의 채널
등을 통해 조치 요청

신고/문의 창구 예시

고객 센터 (Help Center)
문제 신고 양식 제출(Form)



서비스 내 피드백 / 답변 신고 기능

07

AI 서비스에서 플러그인이나 외부 서비스 연동 기능을 사용할 때, 제 데이터는 안전한가요?

- 생성형 AI가 다른 앱이나 외부 서비스와 연결되면 일정 관리, 회의록 정리, 상품 추천 등 더 다양한 일을 할 수 있습니다. 이를 보통 **'플러그인'**이나 **'연동 기능'**이라고 부르며, 최근에는 이용자를 대신해 AI가 업무를 처리하는 비서 역할(에이전트)을 할 때 이 기능을 사용합니다.

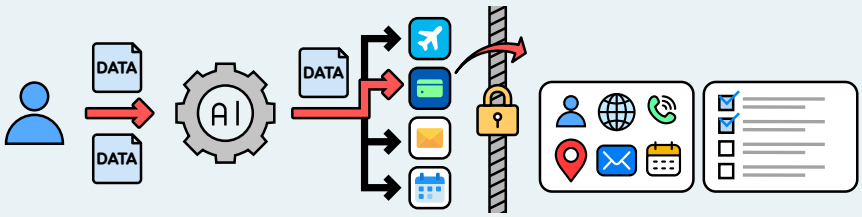
- 편리한 기능이지만 **AI에 입력한 정보가 외부 서비스로 전달**되어 처리되기 때문에 **연동된 외부 서비스가 개인정보를 어떻게 수집·이용·보관하는지 함께 살펴볼 필요**가 있습니다.

- 예를 들어, 여행 예약 서비스와 연결하면 예약 확인을 위해 연락처나 결제 정보가 전달될 수 있습니다. 업무용 도구를 쓸 때는 대화 기록이나 문서 전체에 대한 접근 권한을 요청받기도 합니다. 이 때 전달되는 정보는 연동을 해제하더라도 외부 서비스의 정책에 따라 일정 기간 보관될 수 있습니다.

다만, 이러한 **정보 전달 범위와 처리 과정을 이용자가 일일이 파악하는 데에 어려움**이 있을 수 있습니다. 따라서 **사업자**는 **필요한 범위 내에서만 정보를 요청·처리하고, 이용자가 이해하기 쉽도록 관련 내용을 명확하게 안내할 필요**가 있습니다.

이용자 역시 **연동 기능**을 **사용**할 때는 **권한 요청 내용을 확인**해야 합니다. **기능별·권한별 선택이 가능**하다면 **필요한 범위에서만 연결**하고, **권한 범위가 지나치게 넓다고 판단**되는 경우에는 **해당 연동의 필요성을 다시 확인**하는 것이 좋습니다.

이용자를 위한 똑똑한 관리법



기능별·권한별 선택이 가능하다면 **필요한 범위 내에서만 연결**하고,
과도한 권한을 요구하는 경우 **연동 필요성 다시 확인**하기

08

기사나 블로그처럼 누구나 볼 수 있게 공개된 정보라면, AI 학습 목적으로 사용될 수 있나요?

가능합니다. 하지만, '공개된 정보'라고 해서 무제한으로 쓸 수 있는 것은 아닙니다.
공개된 내용에 이름, 사진, 연락처 등 특정 개인을 알아볼 수 있는 정보가 포함되어 있다면 개인정보에 해당할 수 있으며, 이러한 정보는 법에서 정한 기준과 보호조치에 따라 활용되어야 합니다.

개인정보위는 **「인공지능(AI) 개발·서비스를 위한 공개된 개인정보 처리 안내서('24.7.)」**를 통해 **'정당한 이익'**(개인정보 보호법 §15①6)이 공개된 개인정보 처리를 위한 **실질적인 적법 근거**가 될 수 있다고 판단하고, 해당 조항을 적용할 수 있는 **판단 기준과 요건***을 **구체화**한바 있습니다.

* ❶목적의 정당성, ❷개인정보 처리의 필요성 및 상당성·합리성, ❸구체적 이익형량

따라서 공개된 정보가 AI 학습에 활용되는 경우에도 **법적 요건과 충분한 안전조치가 전제**되어야 하므로, **제한 없이 활용할 수 있는 것은 아닙**니다.

다만 이용자는 **자신이 인터넷에 공개한 정보가 AI 학습에 활용되는 것을 원하지 않을** 수 있습니다. 이 경우 **게시물의 공개 범위를 조정**하거나 **삭제·비공개 설정**을 **활용**할 수 있습니다.

아울러, **플랫폼별 학습 데이터 제외 신청 절차** 등을 확인할 수 있으며, 본인이 운영하는 **웹사이트**나 **블로그**의 경우에는 **AI 크롤러 접근 제한 설정**(robots.txt 등)을 **고려**해 볼 수 있습니다.

이용자를 위한 똑똑한 관리법

01

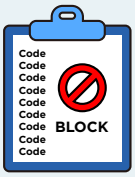
인터넷에 **정보를 공개**할 때, **AI 학습 활용 가능성**도 고려하기

02

게시물 공개 범위와 **삭제·비공개 설정** **주기적으로 확인**하기

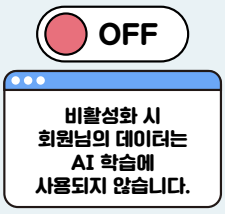
03

학습을 원하지 않는 경우, 학습 제외를 신청하거나 AI 크롤러 접근 제한 설정하기



공개된 정보 관리 방법 예시

게시물 공개범위 설정



학습 데이터 제외 신청

AI 크롤러 접근 제한 설정

기획 및 집필

개인정보보호위원회 인공지능프라이버시팀

AI 프라이버시 민·관 정책협의회 3분과(정보주체 권리)

분과장

-윤혜선(한양대학교 법학전문대학원 교수)

위원

-김근교(NC AI 글로벌사업실장)

-김금선(한국마이크로소프트 변호사)

-김선희(법무법인(유한) 율촌 파트너 변호사)

-김세웅(카카오 부사장)

-김유철(LG AI연구원 부문장)

-서민준(Config 대표이사)

-송현민(단국대학교 사이버보안학과 교수)

-오병일(디지털정의네트워크 대표)

-최홍섭(마음AI 기술총괄 CEO)

-홍준호(성신여자대학교 융합보안공학과 교수)

-황다연(소비자와함께 공동대표/변호사)

* 출처 : 개인정보보호위원회, 「생성형 AI 서비스 이용자를 위한 개인정보 보호 가이드」 2026.5.,
「인공지능(AI) 개발·서비스를 위한 공개된 개인정보 처리 안내서」2024.7.

개인정보보호위원회