

AI 서비스 규제 지도 — AI기본법과 개인정보 보호법이 각각 어디에서 걸리나

이현섭 변호사(법무법인 세움 파트너) · 기준일 2026-09-11 · 최신판: <https://datalaw.kr/guides/ai-basic-law/>

핵심 요약 — AI기본법과 그 시행령은 2026년 1월 22일 함께 시행됐고, 의무 주체인 '인공지능사업자'에는 남이 만든 인공지능을 갖다 써서 제품·서비스를 제공하는 회사도 들어갑니다(법 제2조 제7호 나목). 실무에서 판단이 갈리는 지점은 셋이고 각각 의무의 강도가 다릅니다. ① 우리 인공지능이 고영향에 해당하는지 **사전에 검토하는 것은 의무이고, 과기정통부에 확인을 요청하는 것은 임의입니다**(제33조 제1항). ② 고영향에 해당하면 위험관리방안·설명방안 등 **여섯 가지 조치가 이행 의무로 붙습니다**(제34조 제1항). ③ 기본권 **영향평가는 노력 의무이지만**(제35조 제1항), 국가기관등이 영향평가를 실시한 제품을 우선 고려하므로(같은 조 제2항) 공공조달에 나갈 계획이면 사실상 필요해집니다. 그리고 AI를 붙였다고 AI기본법만 보면 놓칩니다 — 학습 데이터는 저작권법과 개인정보 보호법, 자동화 결정에 대한 이용자 대응은 개인정보 보호법 제37조의2가 따로 겁니다.

☰ **PDF판** — [이 가이드를 PDF로 내려받아](#) 사내·팀에 그대로 전달할 수 있습니다.

AI 규제를 검토해 달라는 요청을 받으면 대개 AI기본법 조문부터 펼쳐게 됩니다. 그런데 실제로 회사가 걸리는 지점은 한 법에 모여 있지 않습니다. 모델을 직접 만들지 않아도 사업자이고, 고영향이 아니어도 투명성 고지는 걸리며, AI기본법을 다 지켜도 학습 데이터와 자동화 결정은 다른 법에서 다시 걸립니다.

이 페이지는 그 조각들을 **판별 순서대로** 묶었습니다. 각 단계에서 어느 글을 읽어야 하는지를 표시해 두었습니다.

1. 우리가 '인공지능사업자'인가

출발점은 수범자 판별입니다. AI기본법의 '인공지능사업자'는 인공지능을 개발해 제공하는 자(가목)와 **그 인공지능을 이용해 제품·서비스를 제공하는 자(나목)**를 모두 포함합니다. 외부 LLM API를 붙인 회사도 여기 들어갑니다.

→ [우리 회사도 '인공지능사업자'인가 — AI기본법 의무 지도](#)

국내에 주소나 영업소가 없는 사업자라면 국내대리인 지정이 따로 걸립니다. 기준은 시행령 제29조 제1항의 네 가지이고, **전체 매출이 작아도 인공지능서비스 부문 매출이 100억 원이면 대상입니다**.

→ [AI기본법 국내대리인 — 전체 매출이 작아도 AI 부문 100억이면 대상입니다](#)

2. 고영향 인공지능인가 — 세 조문이 각각 다른 강도로 걸립니다

여기가 이 법에서 부담이 가장 크게 걸리는 자리입니다. 고영향에 해당하면 책무가 한꺼번에 붙고, 해당하지 않으면 그 부담이 통째로 사라집니다. 판단 대상은 법 제2조 제4호 가목부터 차목까지 열 개 영역이고, 민간 사업자와 가장 넓게 닿는 것은 **사목(채용, 대출 심사 등 개인의 권리·의무 관계에 중대한 영향을 미치는 판단 또는 평가)**입니다.

→ [우리 서비스가 '고영향 인공지능'인가 — 10개 영역과 확인 요청 절차](#)

세 조문이 자주 뭉뚱그려지는데, 의무의 강도가 서로 다릅니다.

조문	무엇을	강도
제33조 제1항	고영향 해당 여부 사전 검토	의무 ("검토하여야 하며")
제33조 제1항	같은 항 뒷부분 — 과기정통부장관에게 확인 요청	임의 ("요청할 수 있다")

조문	무엇을	강도
제34조 제1항	위험관리방안 수립·운영, 설명방안 수립·시행, 이용자 보호방안, 사람의 관리·감독, 조치 내용 문서의 작성·보관 등 여섯 가지 조치	의무 ("이행하여야 한다")
제35조 제1항	기본권 영향평가	노력 의무 ("노력하여야 한다")

실무에서 가장 자주 어긋나는 것이 첫 줄입니다. **확인을 받지 않은 것이 문제가 되는 것이 아니라, 검토를 아예 하지 않은 상태가 조문과 어긋납니다.** 검토 결과 고영향이 아니라는 결론에 이르렀다면 그 판단 근거를 남겨 두는 것이 제33조 제1항에 대한 응답이 됩니다.

제34조 제3항에는 우회로가 하나 있습니다. 다른 법령에 따라 같은 항 각 호에 준하는 조치를 이미 이행한 경우에는 제34조 제1항의 조치를 이행한 것으로 봅니다. 의료기기·금융 등 개별 규제를 이미 받고 있는 회사라면 중복 구축 전에 확인할 자리입니다.

3. 이용자에게 무엇을 고지해야 하나

고영향이 아니어도 대부분의 회사에 걸리는 것이 투명성 의무입니다. 하나의 의무처럼 보이지만 **층이 셋이고, 과태료가 직접 붙는 것은 첫 번째 층뿐입니다.**

→ [첫뿔에 무엇을 고지해야 하나 — AI기본법 제31조의 세 층과 적용 예외](#)

고지는 화면에서 끝나지 않습니다. 프롬프트 입력값을 저장한다면 그것은 처리하는 개인정보의 항목이고, 외부 LLM API를 호출한다면 국외이전이므로 처리방침에 자리가 두 곳 더 생깁니다.

→ [생성형 AI 서비스의 개인정보 처리방침 — 프롬프트 입력값은 어디에 적히나](#)

4. 학습 데이터는 AI기본법 밖에서 걸립니다

학습에 쓴 데이터의 적법성은 AI기본법이 답하지 않습니다. 저작물 쪽은 저작권법이고, 한국에는 TDM 면책 규정이 없어 **적법해 지는 통로가 공정이용(제35조의5) 하나뿐입니다.**

→ [우리가 도입한 AI가 무단 학습을 했다면 책임은 누구에게 있나 — AI 도입 기업의 저작권 리스크](#)

개인정보를 학습에 쓰는 국면은 개인정보 보호법 쪽입니다. 2026년 8월 20일 국회를 통과한 개정안이 인공지능기술 개발을 위한 처리 특례를 신설했는데, **검히는 조문과 그대로 남는 조문이 같습니다 — 국외이전은 남습니다.**

→ [본사가 한국 이용자 데이터로 AI를 학습시키겠다고 합니다 — 새 특례로 검히는 조문과 그대로 남는 국외이전](#)

회사를 사고파는 국면에서는 같은 질문이 자산 실사로 들어옵니다. 데이터 자산이라고 내미는 것을 수집 경로부터 갈라 보는 순서는 아래 글에 있습니다.

→ [대상회사의 데이터 자산, 실사에서 순서대로 묻는 세 질문](#)

5. 개인정보 보호법이 따로 거는 것

AI기본법을 다 지켜도 남는 자리가 있습니다. 자동화된 결정에 대한 이용자의 거부·설명 요구는 개인정보 보호법 제37조의2의 문제이고, 본사 시스템이 내린 결정이라도 **답할 의무자는 한국법인이며 기한이 붙습니다.**

→ [본사 AI가 내린 결정을 한국 이용자가 거부했습니다 — 답할 의무는 한국법인에 있고, 시계는 30일입니다](#)

편향 점검은 방향이 반대로 어긋나는 자리입니다. EU AI Act는 고위험 AI의 편향 탐지를 위해 특별범주 정보의 예외적 처리를 허용하지만, **한국 개인정보 보호법 제23조 제1항에는 그런 예외가 없습니다.** 본사 절차를 그대로 옮기면 점검 자체가 위반이 될 수 있습니다.

→ [본사가 채용 AI의 편향을 민감정보로 점검하고 있습니다 — 한국 법인도 같은 점검을 할 수 있나](#)

처리방침에 새로 채워야 하는 칸이 무엇인지는 아래 글의 항목표에서 확인할 수 있습니다.

→ [개인정보처리방침 필수 기재사항 — 2026년 기준 15개 항목과 2023년 이후 늘어난 것](#)

6. 공공기관에 납품한다면

2026년 7월 21일 시행된 개정 AI기본법으로 국가기관등은 구매·발주 시 AI 제품·서비스를 우선적으로 고려해야 합니다(법 제 16조 제3항). 구매 담당자의 배상책임을 고의·중과실이 있는 경우로 좁힌 제4항이 함께 들어와, 담당자가 결재를 미룰 이유가 하나 줄었습니다.

→ [국가기관의 AI 제품 우선구매 고려 의무 — 공공조달에 나가기 전 지도](#)

다만 우선구매 고려의 대상은 **과기정통부장관이 확인한 제품·서비스로 한정됩니다**(시행령 제15조 제4항). 그래서 실무의 출발점은 우선구매 제도가 아니라 확인을 받는 절차입니다.

→ ['AI 제품·서비스 확인'을 받는 법 — 목록화부터 확인서까지, 고시 제2026-50호 읽기](#)

여기에 발주처 쪽 의무가 계약 요구로 넘어옵니다. 「인공지능 및 데이터 기반 행정 활성화에 관한 법률」이 2026년 8월 28일 시행돼 공공기관에 학습용데이터 품질 확보·현황 제출 등의 의무가 붙었고, 납품사에 직접 적용되는 조문은 없지만 **발주처는 그 이행에 필요한 자료와 협조를 계약으로 확보하려 합니다**.

→ [공공기관에 AI를 납품하는 회사가 8월 28일부터 만나게 될 계약 요구](#)

7. 지키지 않으면 무엇이 오나

법이 사업자에게 직접 붙이는 금전 제재는 **과태료 하나뿐이고, 대상이 세 가지로 한정돼 있습니다**(제43조 제1항, 3천만원 이하).

호	위반 조문	내용
1호	제31조 제1항	고영향·생성형 AI에 기반해 운용된다는 사실의 사전 고지 미이행
2호	제36조 제1항	국내대리인 미지정
3호	제40조 제3항	중지명령·시정명령 미이행

AI기본법에는 과징금이 없습니다. 법률 전문에 과징금 조항이 없고, 벌칙(제42조)은 위원회 관계자의 비밀누설을 벌하는 조문이라 사업자 의무와 무관합니다. 개인정보 보호법을 기준으로 위험을 가늠해 온 회사라면 이 차이를 먼저 잡아야 합니다.

그렇다면 나머지 의무는 어떻게 강제되는가가 남습니다. 답은 **사실조사 조문에 있습니다**. 제40조 제1항이 조사 사유를 열거하는데, 그 목록이 제31조 제2항·제3항, 제32조 제1항·제2항, 그리고 **제34조 제1항**입니다. 이 조문들을 위반하면 조사를 받고, 조사 결과 위반이 인정되면 중지·시정명령이 나오며(제40조 제3항), 그 명령을 이행하지 않을 때 비로소 과태료가 붙습니다.

두 조문을 겹쳐 놓으면 의무가 세 층으로 갑니다.

층	조문	위반하면
직접 과태료	제31조 제1항(사전 고지) · 제36조 제1항(국내대리인)	곧바로 과태료
2단 경우	제31조 제2항·제3항(생성형 표시·딥페이크 표시) · 제32조 제1항·제2항(안전성) · 제34조 제1항(고영향 여섯 조치)	사실조사 → 시정명령 → 명령 불이행 시 과태료

층	조문	위반하면
경로 없음	제33조 제1항(고영향 사전 검토) · 제35조 제1항(영향평가)	조사 사유 목록에도 없습니다

세 번째 층을 눈여겨보시기 바랍니다. **제33조 제1항은 문언이 「검토하여야 하며」로 의무인데도 조사·제재로 가는 길이 없고**, 제35조 제1항은 노력 의무인 데다 역시 길이 없습니다. 그렇다고 제35조를 넘길 수는 없습니다 — 같은 조 제2항이 국가기관등에 영향평가 실시 제품을 우선 고려하도록 정해 두었기 때문입니다. **제35조를 움직이는 것은 제재가 아니라 조달입니다.**

정부는 최소 1년 이상의 계도기간을 두어 사실조사와 과태료 부과를 원칙적으로 하지 않겠다고 밝혔습니다. 그러나 **계도기간은 부칙의 적용 유예가 아니라 행정 운영 방침이고, 의무 자체는 2026년 1월 22일부터 발생해 있습니다.** 계도기간의 실제 효과를 읽으려면 위 구조를 먼저 봐야 합니다.

→ [계도기간이니 지금은 안 지켜도 되나 — AI기본법 과태료의 실제 구조](#)

세부 기준은 이미 시행령에 내려와 있습니다

「AI기본법은 아직 세부가 안 나왔다」는 말을 자주 듣지만, 위임 사항은 시행령(대통령령 제36580호, 2026년 8월 20일 시행)에 이미 채워져 있습니다. 개인정보 보호법 쪽은 시행령 개정령이 시행 하루 전인 2026년 9월 10일에야 공포된 것(대통령령 제36671호)과는 반대 상황입니다.

법 조문	위임한 것	받은 시행령 조문
제31조 제4항	고지·표시의 방법과 예외	제23조(인공지능 투명성 확보 의무)
제32조	안전성 확보 조치	제24조(인공지능 안전성 확보 의무)
제33조 제4항	고영향 확인 절차	제25조(확인 절차 등) · 제26조(전문위원회)
제34조 제1항·제3항	여섯 조치의 이행 방법	제27조(고영향 인공지능과 관련한 사업자의 책무)
제35조 제3항	영향평가의 내용·방법	제28조(고영향 인공지능 영향평가)
제36조 제1항	국내대리인 지정 대상 기준	제29조(국내대리인 지정 사업자의 기준)
제43조 제1항	과태료 부과기준	제32조 및 별표 2

이 지도에 아직 없는 것

- **고영향 인공지능 영향평가(제35조)의 구체적 방법.** 법이 내용·방법을 대통령령에 위임하고 시행령 제28조가 그것을 받았습니다(위 7번 표). 다만 민간에는 노력 의무여서 이 지도는 위 2번의 강도 구별과 조달을 통한 강제 구조까지만 다루고 있고, 시행령 제28조를 조문 단위로 읽는 것은 별도의 글로 정리할 자리입니다.
- **안전성 확보 의무(제32조)의 적용 범위.** 누적 연산량 기준에 걸리는 회사가 매우 제한적이라 이 지도에서는 판별 단계에만 두었습니다. 기준의 근거와 계산 방법은 위 1번의 [의무 지도 글](#)에서 다룹니다.
- **AI기본법 위반의 제재 사례.** 계도기간 중이라 축적된 사례가 없습니다. 개인정보 보호법 쪽 제재는 [제재 추적기](#)에서 조문별로 확인할 수 있습니다.
- **과태료의 실제 금액.** 부과기준은 시행령 별표 2에 있는데 이 지도는 아직 그 금액표를 신지 않았습니다. 상한이 3천만원이라는 것과 별표가 정하는 개별 기준은 다른 이야기이므로, 원문을 확인한 뒤에 넣겠습니다.

자주 묻는 질문

Q. 고영향 인공지능 해당 여부를 과기정통부에 확인받아야 하나요?

확인 요청은 임의입니다. 의무인 것은 확인 요청이 아니라 사전 검토입니다(제33조 제1항, 위 2번).

Q. 고영향 인공지능 영향평가는 반드시 해야 하나요?

민간 사업자에게는 노력 의무입니다(제35조 제1항). 다만 국가기관등이 영향평가를 실시한 제품을 우선 고려하므로(같은 조 제2항), 공공부문 납품을 계획한다면 실질적으로 필요해집니다(위 2번·6번).

Q. AI기본법을 위반하면 과징금이 나오나요?

AI기본법에는 과징금이 없습니다. 사업자에게 붙는 금전 제재는 제43조 제1항의 과태료(3천만원 이하) 하나이고, 대상도 세 가지뿐입니다(위 7번). 벌칙 조항인 제42조는 위원회 관계자의 비밀누설을 벌하는 조문이라 사업자 의무와 무관합니다.

Q. 계도기간이라 지금은 지키지 않아도 되나요?

계도기간은 법령상 유예가 아니라 행정 운영 방침이고, 의무는 2026년 1월 22일부터 발생해 있습니다(위 7번).

관련 가이드

- [2026년 개정 개인정보 보호법 — 9월 11일부터 무엇이 달라졌나](#)
- [위탁·수탁 개인정보 책임 지도 — 우리는 어느 자리에 있나](#)
- [IT·개인정보 법령 시행일 캘린더](#)

이 글은 일반적인 정보 제공을 목적으로 하며, 구체적인 사안에 대한 법률자문이 아닙니다. 개별 사안은 사실관계에 따라 결론이 달라질 수 있으므로 별도의 검토가 필요합니다.

참고 자료

- [인공지능 발전과 신뢰 기반 조성 등에 관한 기본법](#) 제2조(정의), 제16조(인공지능기술 도입·활용 시책 등), 제31조(인공지능 투명성 확보 의무), 제32조(인공지능 안전성 확보 의무), 제33조(고영향 인공지능의 확인), 제34조(고영향 인공지능과 관련한 사업자의 책무), 제35조(고영향 인공지능 영향평가), 제36조(국내대리인 지정), 제43조(과태료) — 국가법령정보센터. 법률 제21311호(2026. 1. 20. 공포, 2026. 7. 21. 시행)
- [인공지능 발전과 신뢰 기반 조성 등에 관한 기본법 시행령](#) — 국가법령정보센터. 대통령령 제36580호(2026. 8. 18. 공포, 2026. 8. 20. 시행)
- [개인정보 보호법](#) 제23조(민감정보의 처리 제한), 제37조의2(자동화된 결정에 대한 정보주체의 권리 등) — 국가법령정보센터
- [인공지능 및 데이터 기반 행정 활성화에 관한 법률](#) — 국가법령정보센터. 법률 제21392호(2026. 8. 28. 시행)

자주 묻는 질문

Q. 고영향 인공지능 해당 여부를 과기정통부에 확인받아야 하나요?

확인 요청은 임의입니다. 의무인 것은 확인 요청이 아니라 사전 검토입니다. 법 제33조 제1항은 인공지능사업자가 자사 인공지능이 고영향에 해당하는지 '사전에 검토하여야 하며, 필요한 경우' 과학기술정보통신부장관에게 확인을 요청할 수 있다고 정합니다. 검토를 아예 하지 않은 상태가 조문과 어긋나는 것이고, 검토 결과 해당하지 않는다는 결론에 이르렀다면 확인을 받지 않아도 됩니다.

Q. 고영향 인공지능 영향평가는 반드시 해야 하나요?

민간 사업자에게는 노력 의무입니다. 법 제35조 제1항은 '평가하기 위하여 노력하여야 한다'고 정합니다. 다만 같은 조 제2항이 국가 기관등으로 하여금 영향평가를 실시한 제품·서비스를 우선적으로 고려하도록 하고 있어, 공공부문 납품을 계획하고 있다면 의무가 아니더라도 실질적으로 필요해집니다.

Q. AI기본법을 위반하면 과징금이 나오나요?

AI기본법에는 과징금이 없습니다. 사업자에게 붙는 금전 제재는 제43조 제1항의 과태료(3천만원 이하) 하나이고, 대상도 세 가지로 한정돼 있습니다 — 제31조 제1항의 사전 고지 미이행, 제36조 제1항의 국내대리인 미지정, 제40조 제3항의 중지·시정명령 미이행입니다. 벌칙 조항인 제42조는 위원회 관계자의 비밀누설을 벌하는 조문이라 사업자 의무와 무관합니다. 개인정보 보호법의 과징금을 기준으로 위험을 가늠해 온 회사라면 이 차이를 먼저 확인하시기 바랍니다.

Q. 계도기간이라 지금은 지키지 않아도 되나요?

계도기간은 부칙의 적용 유예가 아니라 행정 운영 방침입니다. 의무 자체는 2026년 1월 22일부터 발생해 있고, 계도기간은 사실조사와 과태료 부과를 원칙적으로 하지 않겠다는 집행 방침입니다. 그리고 과태료가 직접 붙는 위반은 사전 고지 미이행과 국내대리인 미지정 둘뿐이며, 나머지는 사실조사와 시정명령을 거쳐 그 명령을 이행하지 않을 때 과태료로 이어지는 구조입니다.