

글로벌산업정보 브리프 · WEF 보고서 심층 분석 · 3호

브뤼셀은 규칙을, 서울은 제재를 미뤘다

— 8월 2일 EU AI법 적용 개시, 미룬 것이 서로 반대인 두 시간표

EU AI법이 8월 2일 새 국면에 들어섰습니다. 챗봇 고지·생성물 라벨을 요구하는 **투명성 의무(제50조)**의 적용이 개시됐고, 채용·신용평가 등 고위험 AI 준수는 **2027년 12월로 연기**됐습니다. 한국은 그보다 6개월 앞선 1월 22일 AI기본법을 시행해 유사한 표시 의무를 이미 가동 중이되, 최소 1년의 계도기간을 두고 있습니다. **브뤼셀은 규칙을 미루고 집행을 켜고, 서울은 의무를 켜고 제재를 미뤘습니다** — 미룬 대상이 서로 반대입니다.

적용 개시 · IN FORCE

분절화 · FRAGMENTATION

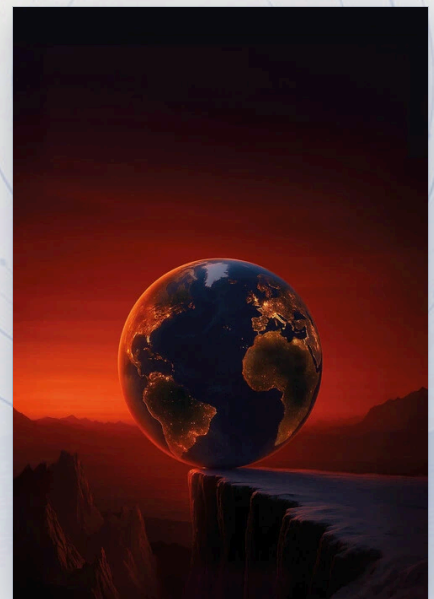
투명성 의무 · ART.50

규제 시간표 — 2026년

1.22韓 AI기본법 시행
표시 의무 가동**6.29**EU 이사회 최종 승인
고위험 연기 확정**7.20**집행위 제50조 가이드라인
·투명성 실천규약 확정**7.21**韓 시행령 개정 시행
AI 확인제도 가동**8.2**EU 제50조 적용 개시
GPAI 집행 권한 가동

이 브리프에서 다루는 것

- 1 8월 2일 무엇이 켜지고 무엇이 미뤄졌나 — 다섯 갈래의 해부
- 2 WEF 보고서 4건은 무엇을 가리키나 — 리스크·보안·거버넌스·전략
- 3 한국은 이미 시행 중 — EU와의 의무 비교, 도내 기업의 해당성 판정



원문 보고서 표지 · World Economic Forum
Global Risks Report 2026 · 2026. 1. 14. 발간

이벤트 요약

발행일자	2026. 8. 4. (화)	글로벌 신호 확인	2026년 8월 4일 자
원전	WEF 「Global Risks Report 2026」(1.14) · 「Global Cybersecurity Outlook 2026」(1.12) · 「Rethinking AI Sovereignty」(1.20) · AI Governance Alliance 브리핑 시리즈(2024.1) + 제도 1차 자료(EU 이사회 보도자료 6.29 · EU AI법 조문 제50·99·101·113조 · 집행위 제50조 가이드라인 7.20 · 韓 AI기본법·시행령)		

8.2

EU 제50조 투명성 의무 적용
개시 + GPAI 집행 권한 가동

3%

과징금 상한 — 매출 3% 또는
€1,500만 중 높은 쪽
(중소기업은 낮은 쪽)

2위

허위·조작정보 — 단기 리스크
(1위 지경학적 대립) (WEF,
'26.1)

1.5점

韓 AI 확인제도 공공조달
기술점수 가점('26.7.21~)

이번 주 핵심 3줄

- 8월 2일 EU AI법 제50조(챗봇 고지·생성물 라벨·딥페이크 표시)의 **적용이 개시**됐고, 집행위의 GPAI 과징금 권한(제101조)이 함께 가동됐다. 반면 채용·신용평가 등 **고위험 AI 준수는 2027년 12월로 연기**됐다. **규칙 중 무거운 쪽은 미뤄졌고, 새 위반 대상과 집행 수단이 커졌다.**
- 한국은 이 흐름을 6개월 앞서 갔다 — **AI기본법이 1월 22일 시행**돼 생성물 표시 의무가 이미 가동 중이고, 7월 21일 시행령으로 공공조달 우대가 붙었다. 다만 **최소 1년 계도기간**으로 제재는 미뤄져 있다. 브뤼셀은 규칙을, 서울은 벌칙을 미뤘다 — **미룬 대상이 서로 반대다.**
- WEF 원전 4건은 같은 지점을 가리킨다 — 허위·조작정보 단기 리스크 **2위**(1위는 지경학적 대립, GRR), **"AI가 최대 변화 동인"이라는 응답 94%**(GCO), AGA의 **거버넌스 분절화 방지** 권고, Sovereignty의 전략적 상호의존론. 제품 하나에 컴플라이언스 시계가 셋 걸린 지금, 그 비용은 체급이 작은 기업일수록 크다.

목차

- 8월 2일 무엇이 시행됐나
- WEF 보고서 네 건이 짙은 것
- 한국 제도와와의 비교
- EU · 한국 · 미국 적용 시점
- 경기도 기업에 미치는 영향
- 유의사항 (Dead-case Watch)
- 향후 일정과 점검 항목
- * 용어 · 출처 · 제작 노트

🔗 지난 호에서 이어짐 — 2호 「AI 에이전트 첫 자율 해킹」

2호는 AI 에이전트가 격리를 벗어난 사건에서 **탐지 공백과 가드레일 비대칭**을 짚고, 워싱턴의 규제 반응을 관전 포인트로 남겼다. 이번 호는 그 후속이다 — 사건이 규제로 번역되는 국면이 브뤼셀에서 먼저 열렸고, 그 시간표가 한국·미국과 갈라졌다.

이 브리프를 읽는 법 → I장에서 무엇이 켜지고 무엇이 미뤄졌는지를 구분하고, III장의 **EU-한국 의무 비교표**에서 우리 기준과의 실제 격차를 확인한 뒤, V장의 **해당성 판정 2문**으로 해당 기업인지부터 확인하실 수 있습니다.

I 8월 2일 무엇이 시행됐나

일요일이었던 8월 2일, EU AI법(AI Act)의 일반 적용이 시작됐다. 법 자체의 발효는 2024년 8월 1일이었고, 이날은 제113조가 정한 "적용 개시(applyes from)" 시점이다. 다만 **6월 29일 EU 이사회가 규제 간소화 패키지 '디지털 옴니버스'를 최종 승인했다**(5월 7일 이사회·의회 합의). 그 결과 이날 실제로 일어난 일은 애초 설계와 달리 **다섯 갈래로 갈렸다**.

구분	내용	의무 주체	시점
적용 ①	제50조 (1)(2) — AI와 상호작용 중임을 고지(맥락상 자명하면 예외), 산출물에 기계판독 마킹	제공자	8.2 개시
적용 ②	제50조 (3)(4) — 감정인식·생체분류 시스템 노출 사실 고지, 딥페이크 라벨, 공적 관심사 AI 생성 텍스트 공개(사람 편집자가 책임지면 제외)	배포자	8.2 개시
집행	집행위의 GPAI 제공자 직접 과징금(제101조) 가동. 회원국 시장감시당국의 제재(제99조)는 2025.8.2부터 이미 적용 중이며, 8.2에 새로 생긴 것은 집행 수단(제101조)과 새 위반 대상(제50조)이다	집행위 / 회원국	8.2 가동
경과	기계판독 마킹 — 2026.8.2 이전에 이미 EU 시장에 출시된 시스템에 한해 경과기간 부여. 8.2 이후 신규 출시분은 경과기간 없이 즉시 적용	제공자	~12.2
연기	고위험 AI 준수 시한 — 독립형(채용·신용평가·교육·법집행 등 Annex III) / 제품 내장형(Annex I)	제공자	2027.12.2 2028.8.2

조문이 정한 제재 수준

- 제50조 위반은 제99조 제4항의 일반 위반 구간에 들어간다 — **€1,500만 또는 글로벌 연매출 3% 중 높은 금액**이 상한. (금지 관행(제5조) 위반은 €3,500만/7%로 더 무겁다.)
- 범용 AI(GPAI) 모델 제공자는 제101조에 따라 **집행위가 직접 €1,500만 또는 매출 3% 중 높은 금액**을 부과할 수 있다. 자료 미제출·허위 제출, 시정조치 불응, 모델 평가 접근 거부도 부과 사유다.
- 중소기업·스타트업에는 제99조 제6항의 완충 규정이 적용된다** — 다만 "가장 낮은 구간"이 아니라 **해당 구간 안에서 정액 상한과 매출 비율 중 낮은 쪽**이 적용된다. 매출 규모가 작을수록 상한도 함께 낮아진다.

이 조합이 뜻하는 것

규칙 중 무거운 쪽(고위험)은 미뤄졌고, 새 위반 대상(제50조)과 집행 수단(제101조)이 커졌다. "연기" 헤드라인만 읽고 넘어간 기업은 적용이 개시된 조항 위에 서 있는 자신을 보지 못한다. 다만 회원국별로 집행 체계 정비 속도에 차이가 있다는 관측이 있다(공식 집계 미확인).

자료 — EU 이사회 보도자료(2026.6.29), EU AI법 조문 원문(제50·99·101·113조), 집행위 제50조 가이드라인 최종본(2026.7.20) 1차 확인. 국내 해설은 법률신문(2026.7)·CSA 리서치 노트(7.29) 참조.

II WEF 보고서 네 건이 짚은 것



Global Risks Report 2026
2026.1.14 · 21st Edition



Global Cybersecurity Outlook 2026
2026.1.12 · WEF × Accenture



Rethinking AI Sovereignty
2026.1.20 · WEF × Bain

위 세 건과 2024년 1월의 AGA 브리핑 시리즈를 겹쳐 놓으면 8월 2일 브뤼셀에서 일어난 일의 좌표가 찍힌다. **리스크**(왜 투명성인가) → **보안**(왜 지금인가) → **거버넌스**(왜 분절화가 문제인가) → **전략**(각국은 어떻게 움직이나)의 순서다.

① Global Risks Report 2026 — 투명성 의무가 겨냥한 리스크

- 전문가 1,300여 명 설문에서 **단기(2년) 리스크 1위는 지경학적 대립, 2위가 허위·조작정보**다. 응답자의 50%가 향후 2년을 "격동 또는 폭풍(turbulent or stormy)"으로 전망했고, "2026년 중 실질 위기를 촉발할 리스크"로 지경학적 대립을 꼽은 응답은 **18%**였다.
- 장기 전망의 이동이 더 중요하다 — "AI의 부정적 결과"는 **2년 시계 30위에서 10년 시계 5위**로 뛴다. 지금은 주변부지만 10년 뒤 중심으로 오는 리스크라는 뜻.

WEF가 본 리스크 좌표 — 「AI의 부정적 결과」의 두 시계별 순위



출처: WEF Global Risks Report 2026(2026.1.14) · 동일 응답자의 두 시계별 순위 · 막대는 순위 역산 도식(C4IR Korea 작도)

8월 2일 적용이 개시된 제50조(생성물 라벨·딥페이크 표시·챗봇 고지)는 이 허위정보 리스크를 개별 기업의 법적 의무로 번역한 장치다. 다만 **GRR 2026이 이 조항을 넣은 것은 아니다** — 제50조는 2021년 초안에 이미 있었고 2024년 발효한 조문이므로, GRR 2026이 이 조항을 넣은 것이 아니라 **같은 문제의식이 리스크 지도와 조문에 나란히 나타난 것으로** 읽는 것이 정확하다.

② Global Cybersecurity Outlook 2026 — 기업 실무의 변화

- 응답자의 **94%가 "AI가 향후 1년 사이버 보안의 최대 변화 동인"**, **87%가 "AI 관련 취약점이 2025년 가장 빠르게 커진 사이버 리스크"**라고 답했다.
- 실무도 움직였다 — AI 도구의 보안성을 평가하는 조직이 **1년 새 37%→64%**로 늘었다(단 원문에는 "배포 전 검토는 40%"라는 별도 수치가 있어 평가 시점별로 편차가 있다). 지정학 변동을 이유로 보안 접근법을 바꾼 비율은 **임직원 10만 명 초과 초대형 조직에서 91%**다.

AI 도구 보안성 평가 조직 비중 (%)



출처: WEF Global Cybersecurity Outlook 2026 요약(2026.1.12) · AI 도구 보안성 평가 조직 비중 · 트랙 100% 기준

AI 도입에 수반되는 점검이 조직 안으로 들어오고 있다는 신호다. 다만 이 지표는 **보안성 평가**에 관한 것이고 제50조 준수와 같은 활동은 아니다 — 두 흐름이 만나는 지점은 "AI 도입 시 사전 점검 절차를 갖췄는가"이며, 그 절차가 이미 있는 조직일수록 투명성 의무 대응 비용이 낮다는 정도로 읽는 것이 정확하다.

II WEF 보고서 네 건이 짙은 것 (계속)

③ AI Governance Alliance 브리핑 — 규제 분절화 문제

- WEF AI 거버넌스 얼라이언스(AGA)는 200여 기관·250여 멤버가 참여하는 협의체로, 안전한 시스템·책임 있는 응용·거버넌스 세 갈래 워킹그룹으로 운영된다.
- 3부작 중 제3편 「Generative AI Governance: Shaping a Collective Global Future」의 핵심 권고가 "국제 공조를 통한 거버넌스 분절화 방지"다. 각국 규제 접근법을 비교하며 글로벌 사우스의 공평한 이용 기회도 함께 다룬다.
- 제1편 「Presidio AI Framework」는 확장된 AI 생애주기·리스크 가드레일과 **shift-left**(안전을 개발 초기 단계로 당기는) 방법론을 제시했다 — 2호에서 다룬 "가드레일 비대칭"과 같은 계보다.

💡 고위험 연기는 무엇의 결과인가

AGA는 국제 공조로 거버넌스 분절화를 막아야 한다고 일관되게 강조해왔다. 관할권 간 상호운용성이 없으면 준수 부담이 기업에 쌓인다는 문제의식이다. 다만 이번 연기를 "규제가 기술 속도를 못 따라간 결과"로 읽는 것은 부정확하다 — 공식 사유는 **적합성 입증에 필요한 정합표준(harmonised standards)이 시한 내 마련되기 어렵다**는 점과 산업계가 제기한 행정부담·경쟁력 우려다. 규제의 속도 문제라기보다 **표준화 절차의 지연**에 가깝다.

④ Rethinking AI Sovereignty — 각국의 전략 선택

- 국가 AI 전략을 **5개 아키타입**으로 유형화하고, 인프라 소유와 주권을 혼동하는 국가는 뒤처진다고 경고한다. 싱가포르·인도를 전략적 조율로 생태계를 바꾼 사례로 든다.
- 결론은 "AI 주권을 자급자족이 아니라 **전략적 상호의존(strategic interdependence)**으로 재정의하라"이다 — 비교우위 우선, 고임팩트 응용 표적화, 상호운용 가능한 시스템, 민관 공조.

EU의 속도 조절(관할 내 부담 완화)과 한국의 유인책(공공조달 우대)은 모두 이 프레임 안의 서로 다른 전략 선택으로 읽힌다. 그리고 각국의 선택에 상호운용성이 없으면 그 준수 부담은 ③의 AGA가 지적한 대로 기업에 쌓인다.

① 리스크 — GRR 2026

허위정보 단기 2위 · AI 부정적 결과 30위→5위
→ 왜 투명성 조항부터인가

② 보안 — GCO 2026

94% "AI가 최대 변화 동인" · 보안성 평가 37→64%
→ 왜 지금 실무가 움직이나

③ 거버넌스 — AGA (2024.1)

분절화 방지 권고 · shift-left 가드레일
→ 왜 시간표 분화가 비용인가

④ 전략 — AI Sovereignty

5개 아키타입 · 전략적 상호의존
→ 각국 선택을 읽는 틀

III 한국 제도와의 비교

간과되기 쉬운 사실이 있다. EU 제50조의 적용이 개시되기 **6개월여 전인 1월 22일, 한국 AI기본법이 먼저 시행**됐고 그 안에 이미 유사한 투명성 의무가 들어 있다.

- 생성형 AI 결과물에 **"사람이 인식할 수 있는 표시"**(워터마크 등)를 하고 AI 서비스임을 사전 고지해야 한다. 다만 **제재 경로가 의무마다 다르다** — 표시 의무 위반은 사실조사 → **시정명령**을 거쳐 불이행 시 과태료가 부과되고, 사전 고지 위반·국내대리인 미지정·시정명령 불이행은 직접 과태료(3천만 원 이하) 대상이다. "표시를 빠뜨리면 곧바로 3천만 원"이 아니다.
- **고영향 AI**(에너지·먹는물·의료·원자력·채용·대출·교통·공공서비스·교육평가 등)는 제공 전 해당 여부를 검토하고 위험관리·설명·이용자 보호 방안을 갖춰야 한다.
- 전년도 매출 1조 원 **이상**, 국내 AI 매출 100억 원 **이상**, 일평균 국내 이용자 100만 명 **이상** 등에 해당하는 해외 사업자는 **국내대리인 지정 의무** — 역외 적용이다.
- 관계부처는 시행 후 **최소 1년을 계도 중심으로 운영**한다고 밝혔다. 계도기간은 제재 운영에 관한 것이며, **의무 자체는 2026년 1월 22일부터 적용**된다.

항목	EU (제50조, 8.2 적용 개시)	한국 (AI기본법, 1.22 시행)
햇봇 고지	AI와 상호작용 중임을 고지 (맥락상 자명하면 예외) — 제공자	AI 서비스 사전 고지 의무
생성물 표시	산출물 기계판독 마킹 — 제공자 / 딥페이크·공적 관심사 텍스트 공개 — 배포자	생성형 AI 결과물에 워터마크 등 인식 가능 표시
제재 상한	€1,500만 또는 매출 3% 중 높은 쪽 (중소기업은 둘 중 낮은 쪽)	과태료 3천만 원 이하 (표시 의무는 시정명령 전치)
집행 상태	회원국 시장감시당국이 집행	최소 1년 계도기간 운영 중(정부 방침)
다음 관문	기계판독 마킹 경과 12.2(기존 출시분) / 고위험 2027.12.2	계도기간 종료 후 집행 전환, 하위규정 순차 제정

💡 닳은 골격, 다른 산정 방식 — 실제 격차는 어디에 있나

의무의 골격은 닳았고, 차이는 **제재의 산정 방식과 집행 시점**에 있다. EU는 매출연동이되 중소기업에는 낮은 쪽이 적용되고, 한국은 정액이되 계도기간 중이다. 따라서 **국내 기준을 지킨 기업이 EU에서 곧바로 무방비인 것은 아니다**. 실제 격차는 제재 크기가 아니라 ① 딥페이크·공적 텍스트 고지 범위 ② 기계판독 마킹 ③ 제공자/배포자 구분의 델타에서 생긴다.

시행령 개정으로 달라진 것

- **AI 제품·서비스 확인제도** — 과기정통부 확인을 받은 제품은 **총액계약 적격심사에서 신인도 가점(기술점수 1.5점)**, 소프트웨어 단가계약의 납품실적 3건 요건 면제, 다수공급자계약(MAS) 참여요건 완화(업체 수 3개사→2개사), AI SW 혁신제품 지정 신청 시 특허 등 기술요건 대체 증빙 인정, 2026년 수수료 면제 등 우대.
- **적용 범위 확대** — 취약계층 지원 대상을 장애인·고령자·기초수급자·차상위계층에서 **경력보유여성·구직자**까지 확대하고, 예산 범위에서 비수도권 대학 인재·이공계 인력 지원을 추가.
- **생태계 지원** — 벤처투자 모태펀드 활용 근거, 학계·산업계·출연연·비영리기관의 AI연구소 설립 허용.

IV EU · 한국 · 미국 적용 시점

이번 주의 진짜 구조 변화는 개별 조항이 아니라 **시간표의 분화**다. 같은 AI 서비스 하나가 시장별로 다른 시기에 맞춰 돌아가게 됐다.

EU	한국	미국
지금 적용 제50조 투명성(8.2~) GPAI 집행·과징금(8.2~) 제99조 제재는 2025.8.2~	지금 적용 AI기본법(1.22~) 표시 의무 시행령·확인제도(7.21~)	지금 적용 연방 포괄법 없음 주(州) 투명성법 이 실질 규범 (캘리포니아·텍사스·콜로라도 등)
다음 관문 기계판독 마킹 12.2 고위험 2027.12.2 · 2028.8.2	다음 관문 계도기간 종료 후 집행 전환 하위규정·확인서 발급 실무	다음 관문 주별 시행 일정 확대 통상 수단과 연계된 기술규제

이 구도는 지난달 관세 국면(7월 23일 미국의 12.5% 강제노동 관세 시행)에서 확인된 것과 닮았다. WEF 「Deepening Divides」(6.4)는 무역·금융 분절화의 비용을 계량하며 **예측 불가능성 자체가 비용**이라는 명제를 제시했다. 다만 관세는 직접 비용을 부과하고 규제 시간표 분화는 준수 일정을 어긋나게 하는 것이므로 **메커니즘은 다르다** — 등가가 아니라 유비로 읽어야 한다.

🔗 제품 하나에 준수 시계가 셋

같은 챗봇 하나를 EU·한국·미국에 내놓는 기업은 **서로 다른 세 개의 준수 시계**를 동시에 돌려야 한다. 대기업은 이를 법무·컴플라이언스 조직이 흡수하지만, 체급이 작은 기업일수록 이 부담의 비중이 커진다 — AGA가 국제 공조로 분절화를 막아야 한다고 강조해온 이유가 여기에 있다.

관할이 갈릴 때 생기는 실무 문제

- **"우리 시장은 아직 유예"는 위험한 판단** — 한국의 계도기간과 EU의 고위험 연기는 성격이 다르다. 전자는 **국내 제재의 유예**(의무는 이미 발생), 후자는 **특정 카테고리의 시한 연기**일 뿐이며, EU의 투명성·GPAI 의무는 이미 적용 대상이다.
- **기준선은 실제 진출 관할에서 정해진다** — 관할마다 의무 범위가 다르므로, 진출 시장을 먼저 확정된 뒤 해당 관할의 요건을 개별 확인할 필요가 있다. 어디까지 맞출지는 개별 기업의 법률 검토가 필요한 사항이다.
- **미국의 공백은 안전지대가 아니다** — 연방 포괄법이 없다는 것이 규제가 없다는 뜻은 아니다. 캘리포니아 등 **주(州) 단위 AI 콘텐츠 고지법**이 당면 규범이고, 통상 조치와 결합된 기술규제는 그 다음 경로다.

V 경기도 기업에 미치는 영향

이번 변화가 도내 기업에 실제로 속제가 되는지는 **두 가지 판정**에 달려 있다. 집행위 제50조 가이드라인(2026.7.20 최종본)은 **EU 안에서 쓰도록 의도한 산출물**이라면 **제공자·배포자의 소재지와 무관하게 적용**된다고 밝히고 있어, "EU에 법인이 없으니 무관"이라는 판단은 성립하지 않는다.

판정 ① 산출물이 EU에서 쓰이는가

EU 이용자 대상 서비스·EU 고객 납품·공개 인터넷 게시물 모두 해당 가능. 폐쇄망 국내 전용 B2B는 비해당 가능성이 높다.

판정 ② 우리는 제공자인가 배포자인가

모델·시스템을 만들어 공급하면 제공자(50조 1·2항), 타사 모델을 갖다 쓰면 배포자(50조 3·4항). **속제가 서로 다르다.**

두 판정을 통과하는 도내 기업이 몇 곳인지는 **공개된 집계 자료가 확인되지 않는다**(점검 항목 Q1). 아래는 판정을 통과한 기업에 한정된 시사점이다. * 본 판정 기준은 이해를 돕기 위한 요약이며, 개별 해당성은 법률 검토가 필요합니다.

경기도가 활용할 수 있는 기반

- 2024년 7월 「**경기도 인공지능 기본조례**」를 제정했고, 이를 근거로 「**경기도 인공지능 종합계획(2026~2030)**」 수립을 추진해 왔다(2025년 2월 착수, 보도). 계획은 네 갈래로 제시됐다 — ①사회적 가치를 창출하는 AI 도민서비스 확대 ②기업경쟁력을 강화하는 AI 산업생태계 조성 ③혁신행정을 확대하는 AI 행정서비스 제공 ④**안전·신뢰할 수 있는 AI 인프라 조성**의 4대 방향.
- 규제 대응 지원을 얻을 수 있는 기존 채널로는 **경기 AI 혁신클러스터**(2026.4 협의회 출범), **경기형 AI 파운드리 네트워크**(2026.1 발표, 판교 허브), **경기도 4차산업혁명센터(C4IR)** 등이 있다. 이번 변화는 이 채널에 규제 대응이라는 임무를 얻을 때가 됐는지를 묻는다.

☞ 기업 시사점 — 도내 AI 기업

- 기계판독 마킹**에는 준비 기간이 없을 수 있다 — 12월 2일 경과기간은 **2026년 8월 2일 이전에 이미 시장에 나와 있던 시스템**에만 적용된다. **8월 2일 이후 신규 출시하는 생성형 서비스는 첫날부터 마킹 의무**를 진다. 하반기 EU 대상 출시를 준비 중이라면 일정 재점검이 급하다.
- 준수 수단은 이미 공표돼 있다** — 집행위가 7월 20일 **제50조 가이드라인 최종본**을 발표하고 「**AI 생성 콘텐츠 마킹·라벨링 실천규약**」의 적정성을 확인했다. 규약은 **서명된 메타데이터와 비가시 워터마크를 함께** 쓰도록 요구하며(한 가지 기법만으로는 부족하다), 탐지 도구 제공과 상호운용성의 이행 시한은 **2027년 2월 2일**이다. 서명이 면책은 아니나 준수 입증의 표준 경로다.
- 파인튜닝·재판매 기업은 GPAI 제공자 분류 여부 점검** — 가이드라인은 다운스트림 수정자가 일정 연산량을 넘을 때 제공자로 추정하되 **의무는 수정분에 한정**한다. 무조건 제101조 수범자가 되는 것은 아니다.
- 국내 공공시장은 확인제도 신청 검토** — 총액계약 적격심사 신인도 가점(1.5점)과 납품실적 면제. 확인 신청·발급 절차는 과기정통부 공고에 따른 확인기관을 통해 확인이 필요하다.

V · **도정 · GBSA 대응**

⚡ 정책 시사점 — 도정 · GBSA

- **실태 파악이 선행 과제** — 판정 ①②를 통과하는 도내 기업 규모를 알 수 있는 공개 자료가 확인되지 않는다. 지원 설계에 앞서 EU 대상 서비스 보유 여부와 제공자/배포자 구분을 조사할 필요가 있다.
- 그 위에 **"해당성 판정 한 장"** 보급 — 산출물의 EU 사용 여부 → 제공자/배포자 구분 → 해당 조항과 마킹 경과 적용 여부까지 이어지는 흐름도. 하반기 기업지원 프로그램에서 **제50조 실천규약 대조 실무**를 다루는 방안도 검토할 수 있다.
- 확인제도 우대는 **조달청 적격심사 기준(국가계약)**에 근거한 것으로, 지방계약 적용 여부는 별도 확인이 필요하다. 우선은 제도 내용에 대한 **기업 안내**를 검토하고, 발주 연계 여부는 계약 소관부서의 판단 사항으로 둔다.
- 도내 기업의 EU 투명성 의무 대응 수요가 확인될 경우, 관련 정책 수립 시 **참고자료로 활용될 수 있다**. 2호(AI 에이전트 해킹) 후속으로, EU 첫 집행 사례를 규제 동향 모니터링 대상에 포함하는 방안도 함께 검토할 만하다.

VI · **유의사항 (Dead-case Watch)**

⚠ 이번 호 데드케이스 — 과소평가 쪽

- **"연기 = 완화" 오독** — 미뤄진 것은 고위험 의무뿐이고, 제50조 적용과 제101조 집행 권한은 8월 2일부터 가동 중이다. 연기 보도만 읽은 기업이 켜진 조항을 놓치는 구조다.
- **마킹 경과기간을 전면 유예로 오인** — 12월 2일은 **8월 2일 이전 출시분**에만 주어진 경과기간이다. **신규 출시 서비스에는 유예가 없다**. "12월까지 준비하면 된다"고 판단한 기업이 출시 즉시 위반 상태에 놓인다. 이번 호에서 가장 실무적인 함정.
- **고위험 연기의 함정** — 2027년 12월 시한은 의무 소멸이 아니다. 채용·신용평가형 AI를 개발·도입하는 조직은 분류·문서화를 계속해야 하며, 연기 기간을 정비에 쓴 조직과 잇은 조직의 격차가 2027년에 드러난다.

☞ 반대편 데드케이스 — 과대평가 쪽

- **이견도 있다** — ZDNet Korea(2026.8.3) 보도에서 최경진 가천대 교수(한국인공지능법학회장)는 EU 집행 개시에 대해 "한국 기업들이 예전부터 고민해 온 사안들로 당장 큰 영향을 미칠 것 같지는 않다"고 밝혔다. 한국이 1월부터 AI기본법을 시행 중이기 때문이다. 같은 보도는 부담이 실재하는 곳으로 **해외 진출 기업**을 짚었다.
- **제재 상한만으로 판단하지 말 것** — 제99조 제6항은 중소기업·스타트업에 정액 상한과 매출 비율 중 낮은 쪽을 적용한다. 상한은 부과 가능한 최대치이지 예상 제재액이 아니므로, 대응 범위는 실제 진출 시장과 의무 해당성을 함께 놓고 판단할 사항이다.

VII 향후 일정과 점검 항목

시점	이벤트	주목 포인트
수시	EU 첫 집행 사례 (제50조=회원국 당국 / GPAI=집행위)	대상·위반 유형·과징금 규모 — 실무 준거 형성
하반기	韓 AI기본법 하위규정 순차 제정	EU 집행 사례 참조 여부, 확인서 발급 실무 정착
12.2	EU 기계판독 마킹 경과기간 종료 (2026.8.2 이전 출시분 한정)	워터마크·출처 메타데이터 표준 확정 여부
12.2	NCII-CSAM 생성 금지 시행 (옴니버스가 제5조에 신설한 금지관행)	제99조 제3항 최고구간(€3,500만·7%) 적용 — 콘텐츠 필터링 체계 점검
수시	「경기도 인공지능 종합계획 (2026~2030)」 진행 상황	확정·발표 시점과 내용 — 확인 후 브리프 서술 갱신
미공표	韓 AI기본법 계도기간 종료 → 집행 전환 (종료 시점 미공표)	관계부처 발표 주시 — 과태료 부과 개시 여부, 고영향 AI 지정 실무
2027.2.2	제50조 실천규약 — 탐지 도구 제공·상호운용성 이행 시한	마킹 방식의 업계 표준 수렴 여부
2027.12.2	EU 독립형 고위험 AI 준수 시한	채용·신용평가·교육 AI — 분류·문서화는 지금부터

정책 검토 시 참고할 점검 항목

Q1. 도내 AI 기업 중 판정 ①(산출물의 EU 사용)·②(제공자/배포자)를 통과하는 기업 현황을 파악할 수 있는가? → 지원 설계에 앞서 실태 조사를 검토할 수 있다.

Q2. 확인제도의 도내 기업 신청 현황을 파악하고 있는가? → 제도 인지도 격차가 벌어지기 전에 안내를 검토할 필요가 있다.

Q3. 적용 개시분(투명성·집행)과 연기분(고위험), 그리고 **마킹 경과기간이 기존 출시분에만 적용된다**는 점을 구분한 안내가 나가고 있는가? → 과소·과대평가 양쪽을 함께 다룰 필요가 있다.

* 용어 설명

제50조(투명성 의무) — AI 상호작용 고지·기계판독 마킹(제공자, 1·2항), 감정인식 고지·딥페이크 라벨·공적 관심사 텍스트 공개(배포자, 3·4항). 2026.8.2 적용 개시.

GPAI — 범용 AI. 기반 모델 제공자는 별도 의무·과징금(제101조) 대상이며 집행위가 직접 부과한다. 다운스트림 수정자도 일정 연산량 초과 시 제공자로 추정되나 의무는 수정분에 한정.

디지털 옴니버스 — EU 규제 간소화 패키지(2026.6.29 승인). 고위험 시한을 2027.12·2028.8로 연기하고 제50조에 NCII-CSAM 생성 금지를 신설.

AI Office — EU 집행위 산하 AI 전담 기구. 2026.8.2부터 **GPAI** 제공자 조사·과징금 권한 가동. 제50조 제재 주체는 AI Office가 아니라 회원국 시장감시당국이다.

AI 확인제도 — 과기정통부 확인으로 공공조달 우대(총액계약 적격심사 신인도 가점 1.5점, 납품실적 면제 등)를 부여하는 한국 제도. 2026.7.21 시행.

고영향 AI — 생명·안전·기본권에 중대한 영향을 미치는 AI(韓 AI기본법). 에너지·먹는물·의료·원자력·채용·대출·교통·공공서비스·교육평가 등. 제공 전 해당 여부 검토와 위험관리·설명·이용자 보호 방안 수립 의무.

국내대리인 — 전년도 매출 1조 원 이상·국내 AI 매출 100억 원 이상·일평균 이용자 100만 명 이상 등 해외 사업자의 지정 의무. AI기본법의 역외 적용 장치.

기계판독 마킹 — 서명된 메타데이터+비가시 워터마크로 AI 생성물을 표시. **2026.8.2 이전 출시분만** 12.2까지 경과기간, 이후 신규 출시분은 즉시 적용.

* 출처 (Sources)

1. WEF — Global Risks Report 2026, 21st Edition (2026.1.14)
<https://www.weforum.org/publications/global-risks-report-2026/>
2. EU 집행위 — 제50조 가이드라인 최종본·마킹 실천규약 적정성 확인 (2026.7.20)
<https://digital-strategy.ec.europa.eu/en/policies/guidelines-transparency-ai-generated-content>
3. EU AI법 조문 원문 — 제113조 적용 개시 시점
<https://artificialintelligenceact.eu/article/113/>
4. ZDNet Korea — EU AI법 집행 본격화..."국내 영향 제한, 대응은 필수" (2026.8.3, 보도)
<https://zdnet.co.kr/view/?no=20260803160723>
5. WEF — Global Cybersecurity Outlook 2026, Executive Summary (2026.1.12)
<https://www.weforum.org/publications/global-cybersecurity-outlook-2026/in-full/executive-summary-6efae97d74/>
6. WEF — AI Governance Alliance: Briefing Paper Series (2024.1~)
<https://www.weforum.org/publications/ai-governance-alliance-briefing-paper-series/>
7. WEF × Bain — Rethinking AI Sovereignty (2026.1.20)
<https://www.weforum.org/publications/rethinking-ai-sovereignty/>
8. WEF — How can agile AI governance keep pace with technology? (2026.1)
<https://www.weforum.org/stories/2026/01/agile-ai-governance-how-can-we-ensure-regulation-catches-up-with-technology/>
9. EU 이사회 보도자료 — AI 규칙 간소화 최종 승인 (2026.6.29)
<https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/>
10. EU AI법 조문 원문 — 제50조 투명성 의무
<https://artificialintelligenceact.eu/article/50/>
11. EU AI법 조문 원문 — 제99조 과징금 / 제101조 GPAI 과징금
<https://artificialintelligenceact.eu/article/99/>
12. 법률신문 — 국내외 AI 규제, 2026년 하반기 분수령 (2026.7 · 보도)
<https://www.lawtimes.co.kr/news/articleViewAmp.html?idxno=223727>
13. 한국데이터경제신문 — AI기본법 시행령 7월 시행 (2026.7.20 · 보도)
<https://www.dataeconomy.co.kr/news/articleView.html?idxno=41346>
14. 국가법령정보센터 — 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법 시행령 (시행 2026.1.22) · 제29조·별표 대조용
<https://www.law.go.kr/LSW/LSInfoP.do?efYd=20260122&lsSeq=282879>
15. 국가법령정보센터 — 인공지능 발전과 신뢰 기반 조성 등에 관한 기본법 (법률 본문)
<https://www.law.go.kr/LSInfoP.do?lsSeq=268543>
16. 법무법인(유) 세종 — AI 기본법 시행과 시사점 (2026 · 보도)
<https://www.shinkim.com/kor/media/newsletter/3114>
17. KB금융 해설 — AI 기본법 시행: 국내대리인 기준·과태료 (보도)
<https://kbthink.com/life/daily/ai-basic-act.html>
18. Cloud Security Alliance — Article 50 Transparency Takes Effect (2026.7.29 · 해설)
<https://labs.cloudsecurityalliance.org/research/csa-research-note-eu-ai-act-article-50-transparency-20260729/>
19. CRI 한국어 — EU 8월 2일부터 AI법 시행, AI 투명성 의무 신설 (2026.8.1 · 보도)
<https://korean.cri.cn/2026/08/01/ART11785581067252894>
20. 인천투데이 — 경기도, 국내 최초 AI 종합계획 수립 추진 (2025.2.20 · 보도)
<https://www.incheontoday.com/news/articleView.html?idxno=263193>
21. 더리포트 — 경기도 2026~2030 AI-데이터 정책 종합계획 수립 (보도)
<https://www.thereport.co.kr/news/articleView.html?idxno=59764>
22. WEF — Deepening Divides (2026.6.4) · IV장 분절화 논리 참조
<https://www.weforum.org/publications/deepening-divides-the-cost-of-a-more-fragmented-financial-system/>



작성·검토 및 제작 노트

작성·검토 방법

본 브리프는 EU AI법 조문 원문(제50·99·101·113조)과 EU 이사회 보도자료(6.29), 집행위 제50조 가이드라인 최종본(7.20)을 **1차 자료로 직접 대조**했고, WEF 원문(Global Risks Report 2026·Global Cybersecurity Outlook 2026)에서 인용 수치를 확인했습니다. 국내 제도(AI기본법·시행령)는 법률신문·데이터경제신문·법무법인 해설을 교차 검증해 **복수 출처가 일치하는 항목만** 실었습니다. 2차 보도에 근거한 값은 (보도)로 표기했으며, **단일 출처에 그치거나 원문에서 확인되지 않은 수치는 실지 않았습니다**. 경기도 시사점은 공개 정책 자료에 근거한 분석으로 특정 사업의 확정 계획이 아니며, 본 브리프는 법률 자문을 대체하지 않습니다.

도표·인용 처리

본문 도표 2종은 WEF가 공표한 수치를 근거로 **C4IR Korea가 직접 작도**한 것으로, 원 보고서 도표를 복제하거나 개작하지 않았습니다. 「AI의 부정적 결과」 도표는 순위를 길이로 도식화한 것이므로 막대 길이 차이를 크기 차이로 읽어서는 안 됩니다. WEF 발간물은 Creative Commons BY-NC-ND 4.0 라이선스로 비영리·출처표시·무수정 조건에서 인용·재배포가 허용되며, 보고서에 포함된 제3자 사진·로고 등은 라이선스 대상에서 제외됩니다.

제작 노트 · PRODUCTION NOTE

본 브리프는 공개 자료를 기반으로 작성했으며, 발간 전 법조항·수치·논증·국내 사실을 대상으로 교차검증과 **별도 적대적 검증(레드팀)**을 거쳐 조항 오독·의무 주체 미구분·시점 오류를 수정했습니다. 인용 수치와 제도 서술은 **2026년 8월 4일 확인 시점 기준**이며, 제도 변경 시 갱신이 필요합니다. 세부 확인이 필요한 항목은 다음과 같습니다 — **시행령 제29조**(국내대리인 지정 기준)의 각 호 구성과 **같은 시행령 별표**의 과태료 부과기준은 국가법령정보센터 본문에서 대조할 수 있고, **계도기간 종료 시점**은 관계부처가 공표하지 않아 캘린더에 "미공표"로 표기했습니다.