Employee AI Use Policies as Compliance Evidence

A Governance Briefing on Article 4, Article 22, and Article 50 Obligations for Deployer Organisations

A Premium AI Governance Desk Briefing for Compliance Officers, HR and Legal Leaders, and AI Governance Teams

Published by AI Governance Desk
Editorial Team: AI Governance Desk
September 2026 Edition

Table of Contents

Key Governance Points: Employee AI Use Policy Obligations in 2026

Key Governance Points

- **Article 4 literacy duty is already enforceable.** AI literacy measures under Article 4 of Regulation (EU) 2024/1689 have applied since 2 February 2025; national market surveillance authorities gained supervisory and enforcement powers over the obligation from 2 August 2026.
- **The Digital Omnibus softened wording, not deadlines.** Regulation (EU) 2026/1744 changed Article 4's standard from “ensuring” to “supporting the development of” AI literacy, but left the applicability date and the August 2026 enforcement start unchanged.
- **Employment-decision AI systems run on a separate, later clock.** Annex III high-risk obligations covering recruitment, task allocation, performance scoring, and termination-related AI systems were deferred from 2 August 2026 to 2 December 2027; embedded Annex I systems move to 2 August 2028.
- **Article 50 transparency duties are live now.** Deployers and providers of AI systems that interact with people, generate synthetic content, or produce content on matters of public interest have carried disclosure obligations since 2 August 2026.
- **Non-compliance carries tiered exposure up to €35 million.** Article 99 sets fines up to €35,000,000 or 7% of global turnover for Article 5 breaches, up to €15,000,000 or 3% for most operator and deployer obligations including Articles 26 and 50, and up to €7,500,000 or 1% for supplying incorrect information to authorities.
- **GDPR obligations attach independently of the AI Act timetable.** Systematic AI-based monitoring of employees triggers a Data Protection Impact Assessment under Article 35 GDPR, and solely automated decisions with legal or similarly significant effect engage the Article 22 GDPR right to human intervention, regardless of any AI Act deferral.

1. Article 4 AI Literacy as a Documented Legal Obligation

Article 4 of Regulation (EU) 2024/1689 requires providers and deployers of AI systems to take measures ensuring, to their best extent, a sufficient level of AI literacy among staff and other people operating AI systems on their behalf. The required level is calibrated to each person's technical knowledge, experience, education and training, and to the context in which the AI system is used and the people it affects. The obligation applies regardless of whether the AI system in question is high-risk, limited-risk, or minimal-risk — it is one of the few duties in the Regulation that reaches every deployer without exception.

The duty has applied since 2 February 2025. What changed on 2 August 2026 is enforcement architecture, not the underlying obligation: national market surveillance authorities gained the formal supervisory and enforcement powers needed to act on non-compliance from that date. Regulation (EU) 2026/1744, the Digital Omnibus on AI, entered into force on 27 July 2026 and revised Article 4's operative verb from “ensuring” a sufficient level of literacy to “supporting the development of” it — a materially softer standard of effort — but did not move the applicability date or the August 2026 enforcement start.

For an organisation building an acceptable use policy, this sequencing matters. The policy itself, together with role-based training records and an acknowledgment log, is one of the few artefacts that demonstrates measures were taken. A policy that exists only as an undated onboarding attachment, with no record of who received which version and when, is difficult to present as evidence of an ongoing measure rather than a one-time notice.

Governance Gap: Article 4 Carries No Standalone EU-Level Fine

- Article 4 is not listed among the fineable provisions in Article 99(3) to (5): unlike Articles 5, 26 and 50, a literacy failure on its own does not trigger one of the Regulation's fixed EU-wide penalty tiers. Exposure instead runs through Article 99(1), under which each Member State sets its own penalty rules for infringements not otherwise covered, and through the role a documented literacy gap can play as an aggravating factor once a regulator is already examining another AI Act matter. That absence of a direct EU-level fine is precisely why the evidentiary record described below carries more weight than it would for a directly sanctioned obligation: it is the primary lever available if enforcement action follows.

Governance Implications

- **Version control:** maintain a dated revision history for the policy document itself, not only for the tools it references.
- **Acknowledgment logging:** record acknowledgment at the individual employee level, tied to the specific policy version they received.
- **Role calibration:** document that literacy measures vary by role and by the AI systems each group actually uses, reflecting Article 4's proportionality standard.
- **Review cadence:** tie policy review to vendor and procurement events, not solely to a fixed annual calendar.

2. The Scope Boundary: General AI Use versus Annex III Employment Decisions

Two distinct obligations are frequently compressed into a single acceptable use document. General employee use of AI tools — drafting assistants, meeting summarisers, coding copilots — sits under the Article 4 literacy duty described above, which is applicable now. AI systems used to make or materially inform decisions about employees — recruitment screening, task allocation, performance scoring, and promotion or termination recommendations — fall under Annex III of Regulation (EU) 2024/1689, which classifies employment-related AI as high-risk.

Regulation (EU) 2026/1744 deferred the Annex III compliance timetable for these stand-alone high-risk systems from 2 August 2026 to 2 December 2027. AI systems embedded in products already governed by EU product-safety law (Annex I) move to 2 August 2028. The deferral applies to the conformity assessment, technical documentation, human-oversight design, and post-market monitoring obligations that Annex III classification triggers — it does not touch Article 4, Article 5 prohibited practices, or Article 50 transparency duties, all of which remain on their original timetables.

An acceptable use policy addressed to general staff does not, and is not intended to, satisfy Annex III. Where an organisation already deploys an AI system to score, rank, or flag employees, that deployment needs its own compliance track: a documented human oversight mechanism, a risk management file, and — independently of the AI Act timetable — the data protection assessment described in Section 4 below.

Compliance Risk: Deferral Does Not Mean No Exposure

- The Digital Omnibus deferral applies to AI Act Annex III obligations specifically. It has no effect on GDPR, which is a separate legal regime. An employer running an AI-based performance-scoring or monitoring tool today is not shielded from Article 22 or Article 35 GDPR exposure by the fact that Annex III enforcement does not begin until 2 December 2027.

3. Tool Governance and Article 50 Transparency Exposure

Article 50 sets transparency obligations that apply independently of an AI system's risk tier. Systems that interact directly with people, generate or manipulate synthetic image, video, audio or text, or produce content published on matters of public interest carry disclosure duties that became applicable on 2 August 2026. The European Commission's guidelines on implementing these obligations, published 20 July 2026, clarify that individual employees using an employer-provided AI tool are not treated as separate deployers: the employer organisation carries the Article 50(3) and 50(4) deployer duties, not the individual staff member using the tool day to day.

That clarification reframes the “approved tools” section of a policy from a list of dos and don’ts for individual staff into a mapping exercise owned by the organisation: which approved tools produce output capable of reaching an external audience without disclosure, and who signs off on that disclosure before publication. Tiering approved tools by data-training terms and by Article 50 exposure gives the policy an actual decision rule rather than a static list that goes stale at the next vendor terms update.

Tier	Typical Use Case	Governing Question
Approved, unrestricted	Internal drafting, brainstorming, code assistance	Does the account tier exclude prompts from model training?
Approved, disclosure required	External-facing content, synthetic media, public-interest text	Does Article 50 disclosure apply before publication?
Restricted, approval required	Tools processing customer or employee personal data	Has a Data Protection Impact Assessment been completed?
Prohibited	Unvetted consumer tools with no enterprise data terms	No basis exists to answer the questions above

Tiering logic derived from Regulation (EU) 2024/1689, Article 50, and the European Commission's 20 July 2026 transparency guidelines. Verify current vendor terms before assigning a tier.

Governance Implications

- **Named ownership:** assign a specific role — not “IT” generally — responsible for classifying each new tool before it is approved.
- **Procurement trigger:** update the tool list whenever a vendor changes its default data-training or retention terms, not on a fixed annual schedule.
- **Disclosure sign-off:** require a named approver for any AI-generated content intended for external or public-interest publication.

4. Data Protection Triggers Under GDPR Articles 6, 22 and 35

Input classification only functions as a usable rule if its boundaries trace back to a legal trigger rather than a subjective sensitivity judgment. Two points anchor the restricted and prohibited tiers of an acceptable use policy directly in data protection law. First, consent is not the applicable legal basis for AI tools involving the monitoring or profiling of employees, given the structural power imbalance inherent in an employment relationship; legitimate interest under Article 6(1)(f) GDPR, supported by a documented three-part test — identifying the interest, establishing necessity, and balancing it against the employee's rights and freedoms — is the basis organisations typically rely on for this category of processing.

Second, systematic monitoring carried out through an AI tool triggers the requirement for a Data Protection Impact Assessment under Article 35 GDPR before the tool is authorised for that purpose, not after it has already been deployed. The European Data Protection Board's guidance on automated decision-making and profiling sets out the standard for when human involvement in a decision is substantive rather than a formal sign-off on an outcome the system has already determined — a distinction that matters directly for any AI tool positioned as merely “assisting” a human reviewer.

Framed this way, a policy stops asking employees to judge sensitivity in the abstract and instead states a fixed rule: personal data connected to monitoring, profiling, or evaluating colleagues does not go into an AI tool until the DPIA and the documented legal-basis assessment exist. General research, sanitised internal drafts, and public information sit in the tiers below that line.

Compliance Risk: Consent Used as the Legal Basis for Monitoring Tools

- Presenting an AI monitoring or profiling tool to staff as something they can “opt into” does not, on its own, establish a valid legal basis under GDPR. Where refusal carries any real or perceived career consequence, consent is unlikely to meet the freely-given standard the Regulation requires, leaving the processing without a defensible basis until legitimate interest is properly documented instead.

5. Enforcement Exposure: Article 99 and GDPR Article 83 Penalty Tiers

Article 99 of Regulation (EU) 2024/1689 sets a three-tier penalty structure. Non-compliance with the prohibited practices in Article 5 — which include, among other listed practices, AI-based inference of employee emotions in the workplace without a medical or safety justification — carries fines of up to €35,000,000 or 7% of total worldwide annual turnover for the preceding financial year, whichever is higher. Non-compliance with most other operator obligations, including deployer duties under Article 26 and transparency duties under Article 50, carries fines of up to €15,000,000 or 3% of turnover. Supplying incorrect, incomplete or misleading information to a notified body or national authority carries fines of up to €7,500,000 or 1% of turnover. For SMEs, including start-ups, each of these ceilings is capped at the lower of the fixed amount or the percentage, rather than the higher.

GDPR runs a parallel and independent penalty structure under Article 83. Failures connected to the lawful basis for processing or to data subject rights sit in the upper tier, with fines of up to €20,000,000 or 4% of global annual turnover. Failures connected to controller and processor obligations — including the Article 35 DPIA requirement discussed in Section 4 — sit in the lower tier, with fines of up to €10,000,000 or 2% of turnover. Because the two regimes are enforced separately, a single AI deployment failure can, in principle, expose an organisation to assessment under both frameworks at once.

Provision	Ceiling	What It Covers
AI Act Art. 99(3)	€35M or 7% turnover	Article 5 prohibited practices
AI Act Art. 99(4)	€15M or 3% turnover	Most operator obligations, incl. Art. 26 deployer duties and Art. 50 transparency
AI Act Art. 99(5)	€7.5M or 1% turnover	Incorrect or misleading information to authorities
GDPR Art. 83(5)	€20M or 4% turnover	Lawful-basis and data-subject-rights failures
GDPR Art. 83(4)	€10M or 2% turnover	Controller/processor obligations, incl. Article 35 DPIA failures

Figures reflect the fixed text of Regulation (EU) 2024/1689, Article 99, and Regulation (EU) 2016/679, Article 83. AI Act SME and start-up fines are capped at the lower, not higher, of the two figures under Article 99(6).

Governance Implications

- **Dual-framework awareness:** assess any AI-based HR or monitoring tool against both AI Act and GDPR exposure, not one in isolation.
- **Documentation as mitigation:** a documented DPIA, legal-basis test, and acknowledgment log are the artefacts regulators look for before considering the higher end of either penalty range.

Implementation Checklist: Building an Evidence-Grade Employee AI Use Policy

The steps below sequence the obligations addressed in this briefing into an order an organisation can reasonably execute, with a named owner and the evidence each step should leave behind.

#	Action	Owner	Evidence Produced
1	Inventory all AI tools in active use, including employee-introduced tools	IT / Procurement	AI tool register
2	Classify each tool by data-training terms and Article 50 disclosure exposure	Governance lead	Tiered tool list
3	Separate general-use tools from any AI system used to score, rank or decide about employees	HR + Legal	Annex III applicability memo
4	Complete a DPIA for any tool involving systematic monitoring or profiling	Data Protection Officer	Signed DPIA, pre-deployment
5	Draft policy sections mapped to Article 4, Article 22 and Article 35	Governance lead	Versioned policy document
6	Distribute the policy and log acknowledgment from every employee with AI access	HR	Acknowledgment log
7	Name the decision types requiring documented human review before acting on AI output	Legal + business owners	Reviewed-decision register
8	Link policy violations to the existing AI/data incident reporting channel	Security / Compliance	Incident procedure cross-reference
9	Set review triggers tied to vendor term changes and the 2 December 2027 Annex III date	Governance lead	Review log with trigger conditions

Sequence steps 1-4 before distributing the policy in step 5; the classification and DPIA work determines what the policy can accurately state.

Sources & Disclaimer

A. Official Regulatory & Government Sources

• European Parliament & Council of the European Union — Regulation (EU) 2024/1689 (Artificial Intelligence Act), full consolidated text, eur-lex.europa.eu/eli/reg/2024/1689/oj/eng, accessed September 2026.

• European Parliament & Council of the European Union — Regulation (EU) 2026/1744 (Digital Omnibus on AI), eur-lex.europa.eu/eli/reg/2026/1744/oj, accessed September 2026.

• European Commission — AI Act Service Desk, Article 4 (AI literacy), ai-act-service-desk.ec.europa.eu/en/ai-act/article-4, accessed September 2026.

• European Commission — AI Act Service Desk, Article 99 (Penalties), ai-act-service-desk.ec.europa.eu/en/ai-act/article-99, accessed September 2026.

• European Commission — Guidelines on transparency obligations for providers and deployers of AI systems (Article 50), published 20 July 2026, digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems, accessed September 2026.

• European Parliament & Council of the European Union — Regulation (EU) 2016/679 (General Data Protection Regulation), eur-lex.europa.eu/eli/reg/2016/679/oj, accessed September 2026.

B. Standards & Frameworks

• National Institute of Standards and Technology (NIST) — AI Risk Management Framework, nist.gov/itl/ai-risk-management-framework, accessed September 2026.

• European Data Protection Board — Guidelines: Automated decision-making and profiling, edpb.europa.eu/our-work-tools/our-documents/guideline/automated-decision-making-and-profiling_en, accessed September 2026.

C. International Organisations

• Organisation for Economic Co-operation and Development (OECD) — OECD AI Principles, oecd.ai/en/ai-principles, accessed September 2026.

D. Established Policy Media & Research

• Gibson Dunn — “EU AI Act Omnibus Agreement — Postponed High-Risk Deadlines and Other Key Changes,” gibsondunn.com/eu-ai-act-omnibus-agreement-postponed-high-risk-deadlines-and-other-key-changes, accessed September 2026.

• Cloud Security Alliance — “EU AI Act's High-Risk Deadline: Deferred, Not Cancelled,” research note, labs.cloudsecurityalliance.org/research/csa-research-note-eu-ai-act-high-risk-deadline-omnibus-20260, accessed September 2026.

E. Tools & Platforms Referenced

• No specific commercial AI tool or vendor platform is named or endorsed in this briefing; the tiering framework in Section 3 is vendor-neutral by design.

Disclaimer

This guide is for informational purposes only and reflects publicly available information as of September 2026. AI laws, regulatory interpretations, technical standards, enforcement priorities, and institutional governance practices may change. Readers should verify current requirements through official regulatory sources, standards bodies, legal advisors, compliance professionals, or qualified governance specialists before making decisions. AIGovernanceDesk.com and its editorial team are not liable for decisions made based on this material. This document does not constitute legal, regulatory, technical, or compliance advice.

Website: aigovernancedesk.com | Email: hello@aigovernancedesk.com | Published: September 2026 Edition

Thank you for reading.

For more governance briefings, visit aigovernancedesk.com

AI GOVERNANCE DESK