opstream

COMPLIANCE RESOURCE

EU AI Act Compliance Checklist

Transparency and GPAI enforcement is live as of August 2, 2026. High-risk obligations land December 2027. This 10-page action plan covers what to do now, what to ask your vendors, and how to build governance before the next deadline.

Aug 2, 2026
Transparency + GPAI enforcement now live

€35M
Max penalty for prohibited AI practices

Dec 2, 2027
High-risk Annex III compliance deadline

Article 26
Deployer obligations now legally binding

Enforcement is live. Belgium issued a €4.2M fine for misclassified biometric AI. Germany and France have opened formal investigations. As of August 2, 2026: Article 50 transparency obligations, GPAI enforcement powers, AI literacy supervision, and AI Office penalty authority are all in effect. The Digital Omnibus defers high-risk Annex III obligations to Dec 2, 2027 and Annex I to Aug 2, 2028. Two new Article 5 prohibitions (non-consensual intimate imagery AI, CSAM generation) take effect Dec 2, 2026.

1 Article 26 Deployer Obligations

Seven legally binding obligations for any organization that deploys a high-risk AI system within the EU. These apply regardless of the Digital Omnibus deferral.

ITEM	OWNER	STATUS
☐ **Follow provider instructions**: Document adherence; off-label use shifts liability	Procurement	
☐ **Implement human oversight**: Assign trained personnel with intervention authority	Executive Sponsor	
☐ **Manage input data quality**: Ensure relevance and accuracy of data entering the system	Data/IT	
☐ **Maintain audit logs**: Retain minimum 6 months; verify SaaS contracts grant export rights	Legal + IT	
☐ **Notify affected individuals**: Disclose high-risk AI decisions to affected people	Legal + HR	
☐ **Notify workers**: Inform workers and representatives before deploying workplace AI	HR + Legal	
☐ **Report incidents**: Document serious malfunctions to providers and authorities within 15 days	Compliance	

> **Opstream tip:** Build an AI Vendor Assessment request type in the Schema Editor. Use vendor questionnaires to collect Article 26 disclosures directly from each vendor through a structured portal.

2 Phase 1: Build AI Vendor Inventory (Start Now)

Identify every AI-enabled vendor in your supply chain. This is the foundation for everything else. Target: complete within 30 days.

	ITEM	OWNER	STATUS
☐	Pull all active vendors from contract repositories and ERP		
☐	Identify vendors with AI/ML capabilities (review MSAs, DPAs, AI addenda)		
☐	Send single-question AI disclosure emails to vendors with unclear status		
☐	Create a centralized AI vendor register (vendor name, AI status, data access, risk tier)		
☐	Flag vendors touching HR/employment, credit/financial, biometric, or access control decisions		
☐	Review all contracts signed in the past 24 months for AI language		
☐	Document which data each AI-enabled vendor accesses		
☐	Check vendor chatbot/virtual assistant interfaces for Article 50 disclosure compliance		

> **Opstream tip:** Use vendor attributes to track AI status, risk tier, and data access per vendor. Set up an "AI Disclosure" attribute (Yes/No/Unknown) and filter your vendor list to surface gaps. Opstream's AI Document Comparison can extract AI-use disclosures from vendor contracts automatically.

3 Phase 2: Risk Classification (Next 30 Days)

Classify each AI vendor against the EU AI Act four-tier risk framework.

RISK TIER	DESCRIPTION	EXAMPLES	ACTION REQUIRED
Prohibited	Unacceptable risk, banned	Social scoring, real-time biometric surveillance	Cease use immediately
High-Risk	Significant impact on individuals	HR screening, credit scoring, biometric ID	Full Article 26 compliance, human oversight, audit logs
Limited Risk	Transparency obligations (Art. 50)	Chatbots, emotion recognition, AI-generated content	Disclose AI use to users; mark synthetic content
Minimal Risk	No specific obligations	Spam filters, search optimization	No action required

ITEM	OWNER	STATUS
☐ Classify each AI vendor into the four-tier risk framework		
☐ Identify all high-risk AI systems requiring full Article 26 compliance		
☐ Assign named human oversight leads for each high-risk vendor		
☐ Verify audit log retention and export rights in vendor contracts		
☐ Document incident notification procedures per vendor		
☐ Assess if any vendors fall into prohibited categories		
☐ Verify limited-risk vendors comply with Art. 50 transparency (chatbot disclosure, content marking)		

Opstream tip: Create custom statuses like "AI Risk: High", "AI Risk: Limited", "AI Risk: Minimal" to track classification progress across your vendor portfolio. Use analytics dashboards to monitor completion rates.

4 Phase 3: Governance Structure (By Q4 2026)

Embed AI compliance into your procurement and legal operating rhythm. Reference the EC's Model Contractual Clauses for AI (MCC-AI) for standard contract language.

ACTION	OWNER	TIMELINE
Add AI disclosure clauses and MCC-AI language to new contracts	Legal + Procurement	Days 1-30
Revise vendor security questionnaires for AI (incl. GPAI Code of Practice)	Procurement + Security	Days 1-30
Assign named oversight leads per high-risk vendor	Executive sponsor	Days 1-60
Confirm log retention and incident notification rights	Legal	Days 1-60
Establish quarterly AI vendor review cadence	GC + C-Suite	Days 1-90
Verify supply chain transparency: vendors disclose AI components to you	Procurement	Days 1-60

ITEM	OWNER	STATUS
☐ Update standard contract templates with AI disclosure clauses and MCC-AI terms		
☐ Add AI-specific questions to vendor security questionnaire (incl. GPAI Code of Practice)		
☐ Confirm oversight personnel have documented intervention authority		
☐ Verify incident reporting procedures for each high-risk vendor		
☐ Schedule quarterly AI vendor review meetings		
☐ Create escalation path for newly discovered AI features in existing vendors		
☐ Document compliance posture for M&A, insurance, and customer due diligence		

Opstream tip: Use automated reminders to trigger quarterly AI vendor reviews. Build a recurring "AI Compliance Review" request type that routes through legal, security, and procurement for each high-risk vendor.

5 AI Literacy (Article 4)

ENFORCEABLE AUG 2, 2026

Every provider and deployer must take measures so staff operating AI systems develop sufficient understanding to use them competently. The Digital Omnibus softened this from an obligation of result ("ensure") to an obligation of effort ("take measures to support"). No specific training program or certification is mandated, but national market surveillance authorities can now supervise and enforce.

ITEM	OWNER	STATUS
☐ **Identify all staff operating AI systems** on behalf of the organization (not just IT)	HR + IT	
☐ **Assess current AI literacy levels** accounting for technical knowledge, experience, education, and context of use	L&D	
☐ **Develop training program** covering AI fundamentals, risk awareness, bias recognition, and human oversight responsibilities	L&D + Legal	
☐ **Train human oversight personnel** for high-risk systems with documented intervention authority and decision-override procedures	Executive Sponsor	
☐ **Document all training measures** taken, including attendance records, materials used, and frequency of updates	HR	
☐ **Consider vulnerable populations** affected by your AI systems when scoping training (e.g., HR teams screening candidates)	Legal + HR	
☐ **Establish refresh cadence** for literacy training as AI tools and regulations evolve	L&D	

> **Opstream tip:** Track AI literacy compliance per team using custom attributes. Create a "Training Status" attribute on vendor records to verify that oversight personnel have completed training before approving high-risk AI vendor requests.

6 Article 50 Transparency Obligations

LIVE AUG 2, 2026

The EU Code of Practice on Marking and Labelling (finalized June 10, 2026) defines exactly how to comply. Penalties: up to €15M or 3% of global turnover. Existing systems get a grace period until December 2, 2026.

OBLIGATION	WHAT IT REQUIRES	KEY DETAIL
Chatbot Disclosure	Users must know they are interacting with AI at the start of each interaction	Use the official EU AI disclosure icon or a capitalized "AI" label "immediately perceivable without user interaction." T&C disclaimers alone do not satisfy.
Synthetic Content	AI-generated content must be marked with at least two methods: metadata + watermarks	Text under 200 tokens is exempt from watermarking. Providers must supply detection tools, generally free of charge.
Deepfakes	Deployers publishing deepfakes on matters of public interest must disclose artificial origin	Disclosure must happen upon first exposure. Intent is irrelevant: content that looks or sounds like a real person must be labeled.
Emotion/Biometric	Deployers of emotion recognition or biometric categorization must inform exposed individuals	Applies to all systems that detect emotions or categorize individuals by biometric data.

ITEM	OWNER	STATUS
☐ **Audit all customer-facing AI touchpoints** for chatbot disclosure compliance (website, apps, email, phone)	Product + Legal	
☐ **Verify vendor chatbots display AI disclosure** before first interaction, not buried in terms	Procurement	
☐ **Implement content marking** for AI-generated text, images, audio, and video (metadata + watermark minimum)	Engineering	
☐ **Label all AI-generated marketing content** published on matters of public interest	Marketing + Legal	
☐ **Document the edited-text exception** where AI-generated text undergoes genuine substantive human editorial review	Legal	
☐ **Plan for interoperability standards** due by February 2, 2027 for content marking	Engineering	

Opstream tip: Add an "AI Transparency Status" field to vendor questionnaires. Use Opstream's approval workflows to block vendor renewals until chatbot disclosure and content marking compliance are confirmed.

7 GPAI Vendor Compliance Questions

The GPAI Code of Practice (finalized July 2025, enforced August 2, 2026) creates three chapters of obligations for providers of general-purpose AI models. Deployers should verify vendor compliance through structured questionnaires. The AI Office can now fine non-compliant providers up to €15M or 3% of global turnover.

Code of Practice Chapters: What to Ask Vendors

Ch. 1: Transparency

Has the provider published model documentation (technical properties, training data, energy consumption, intended use)? Do they respond to downstream information requests within 14 days? Are records maintained for 10 years?

Ch. 2: Copyright

Does the provider maintain a copyright policy with designated oversight personnel? Do they respect robots.txt and machine-readable opt-outs? Do they exclude pirate sites from training data? Have they implemented safeguards against copyright-infringing outputs?

Ch. 3: Safety (Systemic Risk)

For models above 10^{23} FLOP: has the provider established a safety framework? Do they conduct systemic risk analysis? Do they report serious incidents to the AI Office? Do they maintain Safety and Security Model Reports?

ITEM	OWNER	STATUS
☐ **Identify all vendors using GPAI models** (ChatGPT, Claude, Gemini, Llama, Mistral, or any foundation model)	IT + Procurement	
☐ **Add GPAI Code of Practice questions** to vendor security questionnaires (transparency, copyright, safety)	Procurement	
☐ **Request model documentation** from each GPAI provider (model card, technical specs, training data summary)	Legal + IT	
☐ **Verify copyright compliance** for any vendor whose GPAI output your organization publishes or distributes	Legal	
☐ **For systemic-risk models:** confirm the provider has filed a safety framework with the AI Office	Security + Legal	
☐ **Check Code of Practice signatory status** (non-signatories must demonstrate compliance through other means)	Procurement	

Opstream tip: Create a "GPAI Vendor Assessment" request type with vendor questionnaire tabs mapping to each Code of Practice chapter. Use AI Document Comparison to extract GPAI disclosures from vendor documentation automatically.

8 Sector-Specific Obligations

High-risk classification depends on sector and use case. These are the most common categories for deployers. High-risk obligations are deferred to December 2, 2027 (Annex III) and August 2, 2028 (Annex I) per the Digital Omnibus.

Financial Services

High-risk: Credit scoring (Annex III 5(b)), life/health insurance risk assessment (5(c)). Sector regulators (EBA, ESMA, EIOPA) plus national authorities oversee compliance. Customers retain rights to human review, explanation, and contestation of AI-driven decisions. **Deadline: Dec 2, 2027.**

HR / Employment

High-risk: Recruitment, CV screening, targeted job ads, performance monitoring, promotion/termination. Employers must provide human oversight with trained supervisors who retain "effective capacity to intervene." Workers must be informed before deployment. **Deadline: Dec 2, 2027.**

Healthcare / Medical Devices

High-risk: AI in MDR/IVDR-regulated devices is automatically high-risk. ~75% of commercial AI medical devices (mostly radiology, Class IIa+) affected. AI Act layers on top of existing MDR/IVDR obligations. **Deadline: Aug 2, 2028** (Annex I).

The Article 25 Reclassification Trap

A deployer becomes a **full provider** (with conformity assessment, CE marking, and Article 16 obligations) if it:

Rebrands
Puts the AI system on the market under its own name or trademark

Substantially Modifies
Fine-tunes on own data, adds new use cases, or integrates into a pipeline that materially changes function

Changes Purpose
Modifies the intended purpose to make a non-high-risk system high-risk

Phase 4: December 2027 Annex III Transition

Use the deferral period to prepare. Do not wait for the deadline.

ACTION	TIMELINE
Complete high-risk classification for all Annex III use cases	By Q1 2027
Prepare conformity assessment documentation for high-risk systems	By Q2 2027
Engage notified bodies for third-party audit (if required)	By Q2 2027
Implement data governance and quality management systems	By Q3 2027
Register high-risk AI systems in the EU database	By Nov 2027

Opstream tip: Use Opstream's analytics dashboards to track which vendors fall into Annex III categories. Set automated alerts for the December 2, 2027 deadline with 6-month and 3-month advance reminders routed to legal and compliance.

Penalty Reference

Prohibited practices	**€35M or 7% global turnover**
High-risk system violations	**€15M or 3% global turnover**
Supply chain transparency	**€15M or 3% global turnover**
Incorrect/misleading info	**€7.5M or 1% global turnover**
For a $200M company	**$6M per violation (lower tier)**

First Enforcement Cases (2026)

Belgium: €4.2M fine for misclassified biometric AI in warehouse access

Germany: Investigation into recruitment AI vendor for systematic candidate disadvantage

France: Bank credit scoring AI under examination for Article 13 transparency failures

Key Dates (Post-Omnibus)

Aug 2, 2026	Transparency, GPAI, AI literacy enforcement
Dec 2, 2026	New Art. 5 prohibitions (intimate imagery, CSAM AI)
Feb 2, 2027	Content marking interoperability standards
Dec 2, 2027	High-risk Annex III obligations
Aug 2, 2028	High-risk Annex I obligations

Non-Regulatory Pressure Points

Enterprise customer diligence

AI questionnaires alongside security reviews are now standard in enterprise procurement.

M&A and fundraising

AI vendor inventories are now expected in data room due diligence for acquisitions and funding rounds.

Insurance requirements

AI exposure documentation is increasingly required for cyber and professional liability policies.

Best Practices

Start with contracts

Contract repositories reveal AI exposure faster than app catalogs. Review MSAs and DPAs first.

Focus on high-risk first

Apply the 80/20 rule. Full compliance effort on the vendors with the greatest impact on individuals.

Use MCC-AI clauses

The EC's Model Contractual Clauses for AI provide standard language. Available in 24 EU languages.

Automate recurring reviews

Quarterly AI vendor reviews should be automated with reminders, not dependent on manual tracking.

Automate EU AI Act vendor compliance

Inventory, classify, and govern AI vendors in one platform.

Book a Demo