EU AI ACT GUIDE

The EU AI Act for Growing Companies: What Leadership Needs to Know

A practical compliance reference for finance and compliance leaders at companies developing or deploying AI in Europe

fortifai

What the EU AI Act Is and Why It Is Different

The EU AI Act is the world's first comprehensive legal framework for artificial intelligence. Adopted by the European Parliament in March 2024 and entering into force in August 2024, it regulates how AI systems are developed, placed on the market, and used across the European Union and EEA.

Unlike ISO 42001 — which is a voluntary management system standard — the EU AI Act is mandatory law with regulatory enforcement and significant financial penalties. It applies regardless of where a company is headquartered, if the AI system affects people in the EU or EEA.

Three things make the EU AI Act different from other compliance frameworks:

Mandatory and Already in Force

Not a future obligation to plan toward but an active legal requirement with live deadlines.

Most Severe Penalty Structure

The most severe of any technology regulation in the EU, exceeding even GDPR for the most serious violations.

Risk-Based Classification

Classifies AI systems by risk level and imposes fundamentally different obligations depending on that classification — your first compliance task is understanding where your AI sits in the framework.

The EU AI Act and Norway — What EEA Companies Need to Know

The EU AI Act is EU legislation. Norway is not an EU member state but is part of the European Economic Area, which means EU internal market legislation applies to Norway through the EEA agreement.

The EU AI Act will be incorporated into Norwegian law via the EEA process. As with NIS2, the transposition timeline for EEA states runs slightly behind EU member states, but the obligations are identical and the direction is clear.

Three reasons Norwegian companies should treat this as active now:

1 Already Subject to EU AI Act Obligations

Any Norwegian company selling AI-enabled products or services into EU member states is already subject to EU AI Act obligations as a provider or deployer operating in the EU market — regardless of EEA transposition status.

2 Supply Chain Pull-In Is Active and Growing

Norwegian companies supplying essential or important entities under NIS2 are already receiving AI governance requirements in procurement processes that reference EU AI Act obligations.

3 Early Preparation Costs Far Less

The cost of early preparation is far lower than the cost of reactive compliance after formal transposition. Norwegian companies that build their AI governance infrastructure now will be ahead of the compliance curve when the Act is formally incorporated into Norwegian law.

Practical advice: treat EU AI Act obligations as active for compliance planning purposes. Conduct your AI system inventory and risk classification now.

fortifai

The Phased Timeline — What Is Already Active

Date	What Becomes Active
August 2024	Act enters into force. General obligations begin.
February 2025	Prohibited AI practices banned. AI literacy obligations active for all deployers.
August 2025	General purpose AI model rules and governance obligations for GPAI providers active.
August 2026	Full high-risk AI system obligations active. Conformity assessments required.
August 2027	Final provisions for certain legacy and embedded AI systems.

The February 2025 deadline is the one most companies have missed. AI literacy obligations — ensuring that staff who use AI tools have sufficient understanding to use them appropriately and recognise their limitations — became active for all deployers in February 2025. If your company uses AI tools in any business process and has not implemented a documented AI literacy programme, you are already non-compliant.

Risk Classification — Where Your AI Sits

Your obligations under the EU AI Act depend entirely on which risk category your AI systems fall into. This is the first compliance decision you need to make.

Risk Level	What It Covers	Your Obligations
Unacceptable — Prohibited	AI that manipulates people subconsciously, exploits vulnerabilities, enables social scoring, real-time biometric surveillance in public spaces	Banned as of February 2025. Do not deploy.
High Risk	AI in hiring, credit scoring, education assessment, critical infrastructure, law enforcement, border control, administration of justice. AI safety components in regulated products.	Full conformity assessment, technical documentation, human oversight, logging, transparency, registration in EU database
Limited Risk	Chatbots, AI-generated content, deepfakes, emotion recognition	Transparency obligations — users must be told they are interacting with AI
Minimal Risk	Spam filters, recommendation engines, most AI-enabled SaaS features	No specific obligations beyond general good practice

The high-risk classification is broader than most companies expect. An HR tool that uses AI to screen CVs or rank candidates is high-risk. A credit decision support tool is high-risk. An AI system used in educational assessment is high-risk. If your product touches hiring, lending, education, or public services — even as a feature rather than the core product — review the high-risk criteria carefully.

General Purpose AI models (GPAI): Foundation models like GPT-4, Claude, Gemini, and Mistral are classified as GPAI under the Act. Their providers face specific obligations from August 2025. As a deployer building on top of these models, you inherit some governance obligations around how you use and document that dependency.

What the EU AI Act Requires From You as Leadership

The Act places explicit obligations on deployers and providers at the organisational level. Article 26 on deployer obligations requires designated human oversight, staff AI literacy, and — for high-risk AI — fundamental rights impact assessments approved at the appropriate level.

These are the key approvals and actions the EU AI Act requires from executive leadership:

What You're Signing or Owning	When	What a Regulator Checks
AI System Inventory and Risk Classification	Before August 2026, ideally now	Complete inventory with classification rationale, named owner, signed off
AI Literacy Policy and Programme	Already active — February 2025	Documented programme, staff completion records, named executive owner
High-Risk AI Conformity Assessment	Before deploying high-risk AI	Assessment completed, signed off, registered where required
Fundamental Rights Impact Assessment	Before deploying high-risk AI affecting people	Documented assessment with named executive sign-off
Human Oversight Policy	Before deploying high-risk AI	Named human overseers, documented escalation thresholds, evidence of operation
Incident Reporting Decision	Within timeframes set by national authority	Named decision-maker, documented assessment, report filed
Post-Market Monitoring Plan	Ongoing for high-risk AI	Documented monitoring methodology, performance data, anomaly response
Annual Review of AI System Classifications	Annually	Evidence that classifications are reviewed as systems and use cases evolve

The fundamental rights impact assessment is the sign-off most CFOs have not encountered before. For any high-risk AI system, the Act requires an assessment of the potential impact on fundamental rights — including non-discrimination, privacy, dignity, and access to essential services. This must be documented, proportionate to the risk, and signed off at an appropriate level. It is not a technical document — it is a governance decision requiring executive accountability.

The AI literacy obligation is already non-compliant for most companies. As of February 2025, deployers must ensure that staff operating or overseeing AI systems have sufficient AI literacy — the knowledge and skills to use AI tools appropriately, recognise their limitations, and understand when human judgement should override AI outputs. This requires a documented programme with named owner and completion records. A general awareness email does not satisfy this obligation.

High-Level Compliance Checklist

Phase 1 — AI System Inventory and Classification

- Build complete AI system inventory — every AI tool, model, API, and automated decision system in your product and operations
- Classify each AI system using the four risk tiers — document the rationale for each classification
- Identify any prohibited AI practices — confirm none are in use
- Identify all high-risk AI applications — these drive your most demanding obligations
- Identify all limited-risk AI applications — transparency obligations apply
- Appoint AI compliance owner with executive sponsor named at board level
- For Norwegian companies: assess which EU-facing activities create immediate EU AI Act obligations regardless of EEA transposition status

Phase 2 — AI Literacy Programme

- Design AI literacy programme appropriate to staff roles — not a one-size-fits-all awareness session
- Cover: what AI the company uses, how it works at a sufficient level, known limitations, when to escalate or override, how to report concerns
- Deliver to all staff who use, oversee, or make decisions based on AI outputs
- Record completion with named owner and date
- Schedule annual refresh and update process
- Leadership sign-off on programme design and completion status

Phase 3 — Policy Documentation

- Draft and approve AI Governance Policy — top management sign-off required
- Draft Human Oversight Policy — who oversees which AI systems, escalation thresholds, override procedures
- Draft AI Incident Reporting Policy — what constitutes a reportable incident, who decides, what the reporting procedure is
- Draft Third-Party AI Provider Policy — how you select, assess, and govern AI model and tool providers
- Update data governance policies for AI-specific data handling obligations
- Obtain formal sign-off from named approver for each document

High-Level Compliance Checklist

Phase 4 — High-Risk AI Obligations

- Complete conformity assessment for each high-risk AI system
- Produce technical documentation for each high-risk system
- Complete fundamental rights impact assessment — executive sign-off required
- Implement and document human oversight mechanisms — named overseers, documented thresholds
- Implement logging and monitoring for high-risk AI outputs
- Register high-risk AI systems in EU database where required
- Establish post-market monitoring plan with performance metrics and anomaly response

Phase 5 — Limited Risk and Transparency

- Implement transparency notices for all chatbot and AI-generated content interfaces
- Ensure users are informed when interacting with AI
- Implement content labelling for AI-generated images, audio, and video where applicable
- Document transparency measures with named owner

Phase 6 — Incident Reporting Framework

- Define what constitutes a reportable serious incident under the EU AI Act
- Document the decision framework — who decides, on what criteria, within what timeframe
- Identify your national competent authority contact details
- Establish incident notification procedure with named decision-maker
- Test the process — run a simulated AI incident notification exercise

Phase 7 — Ongoing Compliance

- Annual review of AI system inventory and risk classifications — systems evolve, classifications must too
- Annual refresh of AI literacy programme
- Annual policy reviews with executive sign-off
- Continuous post-market monitoring for high-risk AI
- Monitor EU AI Act guidance and national transposition updates
- For Norwegian companies: monitor EEA transposition timeline and update compliance programme accordingly

Manual vs. Automated: What Good Looks Like

EU AI Act Requires	Manual Reality	With Governance Automation
AI system inventory with risk classifications	Spreadsheet, incomplete, not updated when new tools added	Live register with tracked classifications and annual review triggers
AI literacy completion records	Email sent, no tracking, no evidence	Structured programme with completion records retrievable on request
Fundamental rights impact assessment with sign-off	Document created once, not updated as system evolves	Version-controlled with re-approval triggers on material change
Human oversight evidence	Process described in policy, no evidence it operates	Logged oversight decisions with timestamped records
Incident reporting framework	No pre-agreed framework, decision made under pressure	Pre-built decision criteria with notification workflow ready
Post-market monitoring for high-risk AI	Manual review, inconsistent, hard to evidence	Continuous monitoring with structured outputs and audit trail

The EU AI Act creates a continuous compliance obligation — AI systems evolve, classifications change, new tools are adopted. Manual compliance frameworks that are accurate at one point become stale within months. Companies that build governance workflows designed for continuous maintenance rather than point-in-time readiness are the ones that handle regulatory scrutiny without scrambling.

fortifai

What the Penalties Look Like

This is the provision that gets board attention fastest — and rightly so.

Prohibited AI Practices

€35 million or 7% of global annual turnover — whichever is higher

High-Risk AI Non-Compliance

€15 million or 3% of global annual turnover — whichever is higher

Incorrect or Misleading Information to Authorities

€7.5 million or 1.5% of global annual turnover — whichever is higher

For SMEs and Startups

The Act specifies that penalties should be proportionate to company size and that SMEs should face the lower of the fixed amount or the turnover percentage. But the percentages remain — and they apply to **global annual turnover**, not EU revenue.

For Norwegian Companies

EEA transposition will carry equivalent enforcement provisions. Additionally, contractual liability from EU customers whose own AI Act compliance depends on their suppliers' governance posture creates commercial risk independent of regulatory enforcement — and this risk is already active.

The AI literacy obligation deserves special attention: non-compliance with the February 2025 AI literacy requirement means companies are already exposed. While enforcement focus in the early period will likely target higher-risk violations, documented non-compliance with a live obligation is not a comfortable position ahead of the high-risk AI deadlines in 2026.

fortifai

How EU AI Act and ISO 42001 Work Together

These two frameworks are designed as complements, not alternatives.

The EU AI Act

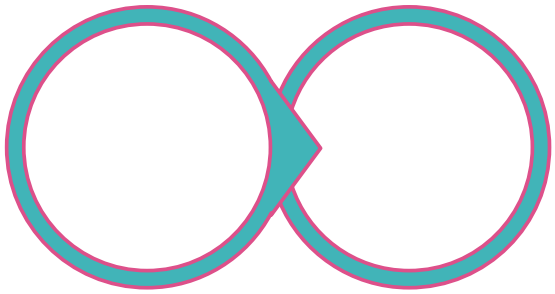
Defines the regulatory obligation — what you must do, by when, under penalty of enforcement. It is the **legal floor**.

ISO 42001

Provides the management system infrastructure to meet those obligations — the documented processes, governance workflows, evidence structures, and continuous improvement mechanisms that prove compliance is operating rather than just stated.

In practical terms: ISO 42001 certification provides documented evidence for many EU AI Act compliance obligations — risk assessments, impact assessments, human oversight mechanisms, incident response, post-market monitoring. Companies pursuing both simultaneously share the governance infrastructure almost entirely, making the combined effort significantly less than the sum of its parts.

> For growing companies facing both obligations, the recommended path is to build the ISO 42001 management system first — it provides the documented governance backbone that EU AI Act compliance evidence sits within.



Building the ISO 42001 management system first creates the shared governance infrastructure that makes EU AI Act compliance materially cheaper and faster to achieve.

How Fortifai Supports This

Fortifai is governance workflow infrastructure built for growing companies. The platform automates the three workflows EU AI Act compliance requires:

Sign-Off Routing and Tracking

For AI policy approvals, classification decisions, and impact assessment sign-offs.

Disclosure Document Management

For conformity assessments, transparency notices, and regulatory submissions.

Information Request Handling

For incident reporting, regulatory evidence requests, and third-party AI provider questionnaires — pre-configured for EU AI Act compliance with templates ready on day one.

The same platform supports ISO 42001, ISO 27001, NIS2, SOC 2, GDPR, and other frameworks simultaneously. For companies managing EU AI Act compliance alongside other regulatory obligations, the governance workflows overlap significantly and the evidence base is shared — making each additional framework materially cheaper than starting from scratch.

> **Book a 30-minute walkthrough at fortifai.co**

fortifai