Roadmap
to comply with
EU-AI act

Made by LE CLUB DPO **in cooperation with the CNIL**

The European Artificial Intelligence Regulation (EU-AI act) represents a major turning point in technology regulation. Adopted in March 2024, this text establishes a binding legal framework for all actors—public and private—who develop, integrate, or use AI systems. This regulatory revolution will be phased in between February 2025 and August 2026/2027, giving organizations a limited window of opportunity to comply.

Governance and management
Structure the organization to anticipate and control

Mapping AI systems
Identify and document the organization's AI ecosystem

Role qualification and responsabilities
Determine responsibilities according to the duties performed

AI act/RGPD Action plan
Integrate compliance procedures in a consistent manner

Risk management
Apply obligations according to risk levels

Accountability and evidence
Demonstrate and maintain compliance over time

CONTEXT

The regulatory context : a revolution underway

The AI Regulation marks a fundamental shift in the European approach to technology regulation. Unlike previous texts, it adopts a particularly broad scope of application, encompassing all AI systems, whether developed in-house, purchased off-the-shelf, or integrated into existing solutions.

This regulation is based on a risk-based approach, establishing differentiated but nonetheless binding obligations depending on the use and risk level of the systems deployed.

This graduated approach allows organizations to focus their efforts on the most critical systems while maintaining an appropriate level of vigilance across their entire AI ecosystem.

The stakes go far beyond simple regulatory compliance.

It is now a strategic imperative affecting brand image, responsible innovation capacity, and competitiveness in European markets. Organizations that anticipate these changes will turn this regulatory constraint into a sustainable competitive advantage.

SCHEDULE FOR ENTRY INTO FORCE

Gradual implementation from February 2025 to August 2026/2027

EXTENDED SCOPE

All AI systems, both internal and external

RISK-BASED APPROACH

Obligations differentiated according to use

ALIGNMENT

Understanding the alignment EU AI act-GDPR

A fundamental distinction must be made: the GDPR regulates personal data, while the EU AI act regulates all AI systems.

These two regulations do not replace each other but complement each other, creating a complex regulatory environment where each text has its own requirements within its area of competence.

This regulatory coexistence means that organizations must now navigate between two complementary approaches: the protection of personal data on the one hand, and the governance of artificial intelligence systems on the other.

The intersection of these two areas creates areas of particular complexity, particularly when AI systems process personal data.

GDPR - Personal Data Protection

- ✓ GDPR - Data Protection
- ✓ Focus on personal data
- ✓ Data Subjects Rights
- ✓ Accountability & documentation
- ✓ DPIA

EU AI Act - AI Governance

- ✓ EU AI act - AI governance
- ✓ Focus on all AI systems
- ✓ Risk-based approach
- ✓ Specific technical requirements
- ✓ Continuous compliance monitoring

The optimal approach is to develop an integrated strategy that addresses both regulations in a consistent manner, identifying potential synergies and avoiding redundancies.

This comprehensive vision will enable DPOs and compliance teams to maximize the effectiveness of their efforts while ensuring complete regulatory coverage.

STEP 1

Governance and management

The establishment of robust governance is the essential foundation of any successful compliance initiative.

This first step involves appointing a manager for the “EU AI Act Compliance” project, who may be the DPO, the CISO, a specialist lawyer, or the head of a dedicated AI unit. This manager must have clear organizational legitimacy and direct access to senior management.

The effectiveness of this governance depends on the creation of a cross-functional project team bringing together essential skills: IT, legal, innovation, and representatives of the business lines using AI.

This diversity of profiles ensures a holistic approach that takes into account all aspects of the issue, from technical constraints to business challenges and regulatory requirements.

Appointment of a pilot

Appoint a manager with a clear letter of assignment defining their role in coordination, arbitration, and reporting to senior management.

Cross-functional team

Set up a working group bringing together IT, legal, innovation, and business departments with a defined committee structure.

Internal roadmap

Establish a provisional schedule with ownerships, deliverables, and kickoff presentation to management.

Team training

Raise awareness among relevant departments about the legal, technical, and ethical issues surrounding AI.

Defining a detailed internal roadmap with a schedule, deliverables, and resource allocation allows this ambition to be transformed into a concrete action plan. This planning must take into account the organization's operational constraints while complying with regulatory deadlines.
Investing in team training is an essential prerequisite for ensuring that all stakeholders understand the issues at stake.

STEP 1

Governance and management

KEY MESSAGE TO TOP-MANAGEMENT

Governing AI means managing risks while anticipating opportunities.

STEP 2

Mapping AI systems

Mapping is the backbone of the compliance process. It aims to comprehensively identify all systems that can be classified as AI systems according to the definition in Article 3 of the AIA. This inventory phase must cover both existing and planned systems, whether they are developed in-house, purchased on the market, or integrated into third-party solutions.

The complexity of this step lies in the need to accurately document the level of risk for each system identified according to the categories established by the Regulation: minimal risk, transparency obligation, high risk, or prohibited systems. This classification directly determines the scope of the applicable obligations and must therefore be carried out with particular rigor.

Comprehensive inventory

Identify all algorithmic systems within the organization and determine which ones fall under the definition of AI according to Article 3 of the IA.

Risk assessment

Classify each system according to four levels: minimal, transparency, high risk, or prohibited. Justify this classification with supporting documentation.

Role assignment

Identify for each system who is the developer, deployer, and other roles according to the definitions in the Regulations.

Mapping must identify general-purpose AI systems and those posing systemic risk, which are subject to specific obligations. Documenting the purposes, data, and their sensitivity under the GDPR makes it possible to anticipate interactions between the two regulations.

This mapping must be kept up to date on an ongoing basis. The rapid evolution of technologies and uses requires constant vigilance to ensure the quality and completeness of information. This implies constant monitoring.

STEP 2

Mapping AI systems

KEY MESSAGE TO TOP-MANAGEMENT

Mapping is like the GDPR: it involves taking stock of the applicable risks and requirements.

Knowing the scope of the task at hand is the basis for any effective action.

STEP 3

Role qualification and responsabilities

The precise definition of roles is a major issue because it directly determines the scope of the obligations applicable to the organization.
The AI Regulation defines five main roles: supplier, deployer, importer, distributor, and agent.
Each role carries specific and cumulative responsibilities, requiring a detailed analysis of the organization's position in the AI value chain.

Provider

Develops or commissions the development of an AI system and markets it under its own name or brand.

Deployer

Uses an AI system under their own authority (excluding non-professional personal use)

Importer, distributor or representative

Is involved in the distribution within the EU of a high-risk AI system bearing the name of a third-party organization outside the EU.

The provider bears the heaviest responsibility: technical compliance, conformity assessment prior to placing on the market, comprehensive technical documentation, CE marking if required, quality management system, post-market surveillance, and corrective measures. These obligations also extend to cooperation with the competent authorities and the appointment of an EU representative if the organization is established outside the Union.

The deployer assumes crucial operational responsibilities: use in accordance with instructions, effective human supervision, verification of input data quality, log retention, reporting of serious incidents, and conducting impact analyses if necessary. These obligations involve a profound transformation of organizational practices and an increase in the skills of user teams.

Responsibilities of the Provider

- ✓ Total technical compliance
- ✓ Prior compliance assessment
- ✓ Detailed technical documentation
- ✓ Quality Management System
- ✓ Post-market surveillance

Responsibilities of the Deployer

- ✓ Use in accordance with instructions
- ✓ Actual human surveillance
- ✓ Data Quality Control
- ✓ Logs retention
- ✓ Team training

The roles of importer, distributor, and authorized representative carry more specific responsibilities. The importer must verify the compliance of imported systems, the distributor ensures that the appropriate documentation is available, while the authorized representative acts as the EU AI act contact point for suppliers based outside the Union.

STEP 3

Role qualification and responsabilities

KEY MESSAGE TO TOP-MANAGEMENT

Everyone has their role, everyone has their responsibilities, and everyone must be aware of them.

STEP 4

Development of the EU-AI act/GDPR action plan

AI quality management

Quality systems for high-risk AI with built-in robustness, security, and traceability

Alert systems

Audit, alert, and withdrawal mechanisms scaled according to risk levels

Integrated documentation

EU-AI act technical documentation combined with GDPR documentation requirements

The EU-AI act/GDPR action plan must establish clear AI governance within the organization, including a steering committee, operational task force, general policy, periodic reviews, and controls.

This must interface effectively with the GDPR organization, clearly defining the role of the DPO in AI projects involving personal data.

Implementing a targeted AI training program is a major strategic investment. It must cover the legal, technical, and ethical aspects of AI while integrating the relevant GDPR dimensions.

The training must be tailored to different profiles and stakeholders.

STEP 4

Development of the EU-AI act/GDPR action plan

KEY MESSAGE TO TOP-MANAGEMENT

The EU-AI act compliance, it's now.

Later, it will be more expensive and potentially too late.

STEP 5

Integrated EU-AI act/GDPR risk management

Risk management is at the operational heart of compliance, requiring a rigorous methodological approach for each AI project.
This approach involves planning a systematic risk analysis that simultaneously integrates the requirements of the AI Act and the GDPR, creating a unified view of compliance issues and enabling optimization of compliance efforts.

The integration of AI risk analyses into existing GDPR impact assessments represents a natural evolution of organizational practices. This convergence avoids duplication of effort while ensuring comprehensive risk coverage.
High-risk AI systems, as defined in accordance with Annex 3 of the AI Act, require special attention with enhanced protective measures.

Risk analysis

Systematic assessment for each AI project incorporating EU-AI act and GDPR

High-risk AI

Identification according to Annex 3 with enhanced protective measures

Privacy by Design

Integration of AI projects into the existing privacy approach

DPO Notice

Systematic consultation for AI systems processing personal data

Data Subject Rights

Anticipating the application of GDPR rights in AI projects

Data breach

Anticipating the consequences on data processed by AI

Integration into the existing Privacy by Design approach is a pragmatic way to capitalize on already established processes. This integration involves systematically consulting the DPO for all AI projects involving personal data, thereby ensuring expert assessment of data protection issues from the design stage onwards.

Anticipating the application of GDPR rights of data subjects in the context of AI represents a major technical and organizational challenge.
The rights of access, rectification, erasure, and portability must be technically feasible even in complex machine learning systems. This requirement imposes specific architectural choices from the design phase onwards.

STEP 5

Integrated EU-AI act/GDPR risk management

KEY MESSAGE TO TOP-MANAGEMENT

Managing your GDPR/AI risks from the outset means ensuring a more secure future.

STEP 6

Accountability and evidence

Integrating proof of compliance into business processes transforms this regulatory constraint into a competitive advantage.
The ability to demonstrate exemplary AI governance becomes a differentiating asset in tenders, contract negotiations, and partner relationships. This added value of compliance more than justifies the investments made.

The establishment of a structured EU-AI act committee with periodic reviews, monitoring dashboards, and reporting to senior management institutionalizes the compliance process. This governance perpetuates compliance efforts and ensures their sustainability over time, even in the event of changes in teams or organizational priorities.

Living documentation

Maintain complete and up-to-date documentation of EU AI act compliance, integrated into operational processes

Audit tooling

Implementation of automated control tools and compliance monitoring dashboards

AI Compliance by Design

Integrating compliance into the design of new systems and processes

Comitology for EU-AI act

Dedicated governance structure with periodic reviews and reporting to management

Integrating proof of compliance into business processes creates a competitive advantage. Demonstrating exemplary AI governance becomes a differentiating asset in tenders and business relationships.
This more than justifies the investments made.
The establishment of an AIA committee with periodic reviews, monitoring dashboards, and reporting to senior management institutionalizes the compliance process. This helps maintain the level of compliance over time.

STEP 6

Accountability and evidence

KEY MESSAGE TO TOP-MANAGEMENT

Compliance is a strategic asset that will distinguish trusted organizations from others in the future.

It's an investment in your sustainability.

ROADMAP

CONCLUSION

At the end of this roadmap, the organization will have a mature and sustainable compliance ecosystem capable of adapting to regulatory and technological changes. This maturity provides a solid foundation for responsible innovation and sustainable growth in tomorrow's digital economy.

LE CLUB DPO

This document was produced by the members of the Club DPO.
More ressources on https://clubdpo.fr