# 📖 Table of Contents

Mamba

# Mamba’s Content Outline

**Article Title:** AI Compliance: What It Is, Why It Matters, and How Organizations Can Prepare (2026 Guide)

**Table of Contents**

# Title & Meta Data

Mamba

# SEO Elements: Title & Meta Data

| ➡️ Title & Meta Data | |
|---|---|
| **Page Type** | New Blog |
| **URL** | /what-is-ai-compliance |
| **Page Title (H1)** | AI Compliance: What It Is, Why It Matters, and How Organizations Can Prepare (2026 Guide) |
| **Meta Title** | AI Compliance: What It Is, Why It Matters, and How to Prepare |
| **Meta Description** | AI compliance ensures AI systems follow laws, ethical standards & rules to protect users, reduce risks & enable responsible innovation. |
| **SERP Intent** | Informational |
| **Keyword Intent** | Informational |
| **Schema Mark Up** | Article |

| ➡️ Author Details [Client to fill] | |
|---|---|
| **Author Name** | |
| **Author Bio** | |
| **Author LinkedIn** | (optional) |

# ✍️ Keywords + Outline

Mamba

| ➡️ Keyword Research | | | | | |
|---|---|---|---|---|---|
| **Type** | **Keyword** | **SV** | **Instances** | **Actual** | **Status** |
| Focus Keyword | ai compliance | 1,300 | 4-5 | | No Instan... |
| Secondary Keyword | ai regulatory compliance | 400 | 2-3 | | No Instan... |
| Secondary Keyword | artificial intelligence regulatory compliance | 150 | 2-3 | | No Instan... |
| Secondary Keyword | regulatory compliance ai | 250 | 2-3 | | No Instan... |
| Secondary Keyword | ai compliance standards | 50 | 2-3 | | No Instan... |

| ➡️ Targeting Details | |
|---|---|
| **Target Product/Solution** | https://www.dpo-consulting.com/ai-act-compliance |
| **Target Persona** | |

| ➡️ Internal Link Recommendations | |
|---|---|
| **Anchor Text + URL** | **Status** |
| • AI Act compliance services [landing] | No Instan... |
| • EU AI Act explained | No Instan... |
| • High-Risk AI Systems | No Instan... |
| • GDPR and AI best practices | No Instan... |
| • DPIA (Data Protection Impact Assessment) | No Instan... |
| • data subject rights | No Instan... |
| • data governance | No Instan... |

**➡️ Competitor References**

- https://www.exin.com/article/ai-compliance-what-it-is-and-why-you-should-care/
- https://www.crowdstrike.com/en-us/cybersecurity-101/artificial-intelligence/ai-compliance/
- https://www.ibm.com/think/insights/ai-compliance
- https://www.gsa.gov/technology/government-it-initiatives/artificial-intelligence/ai-guidance-and-resources/ai-compliance-plan
- https://www.scrut.io/post/ai-compliance

Mamba

# Content Outline

## H1: AI Compliance: What It Is, Why It Matters, and How Organizations Can Prepare (2026 Guide)

---

### H2: TL;DR

---

### H2: What Is AI Compliance?

---

### H2: Why AI Compliance Matters — Regulatory, Ethical, and Operational Drivers

#### H3: Rapid Growth of AI Regulations Worldwide

- EU AI Act
- U.S. AI directives & sector guidance
- UK AI governance frameworks
- Global convergence around risk-based models

#### H3: Business Risks of Non-Compliance

- Reputational credibility
- Legal exposure

- Model failures and operational risk

### H3: The Competitive Advantage of Responsible AI

- Trust, adoption, and user confidence
- Long-term scalability and interoperability

---

## H2: Core Components of an AI Compliance Framework

### H3: Risk Classification and System Categorization

### H3: Data Governance & Dataset Quality Standards

### H3: Transparency, Explainability & Disclosure Obligations

### H3: Human Oversight Mechanisms

### H3: Technical & Cybersecurity Controls for AI Systems

### H3: Monitoring, Logging & Lifecycle Management

---

## H2: AI Compliance Under the EU AI Act (Your Core Service Area)

### H3: Overview of the EU AI Act Requirements

### H3: Obligations for High-Risk AI Systems

### H3: Requirements for General-Purpose AI & Foundation Models

---

Mamba

## H2: AI Compliance in the Context of Data Protection Laws (GDPR, DUAA, PDPL, etc.)

### H3: Lawful Basis for AI Processing Under GDPR

### H3: DPIAs for AI Systems

### H3: Data Subject Rights & Explainability Requirements

- Access, objection, human intervention

---

## H2: Key Challenges Organizations Face When Adopting AI

---

## H2: How to Build an AI Compliance Strategy (Step-by-Step)

### H3: Step 1 — Identify and Classify AI Systems

### H3: Step 2 — Conduct a Gap Assessment Against Applicable Regulations

### H3: Step 3 — Strengthen Governance, Policies, and Risk Controls

### H3: Step 4 — Conduct DPIAs/SIAs and Model Impact Assessments

### H3: Step 5 — Implement Monitoring and Auditing Workflows

### H3: Step 6 — Train Teams Across Technical and Non-Technical Functions

### H3: Step 7 — Prepare for External Scrutiny and Documentation Requirements

---

Mamba

## H2: AI Compliance Use Cases Across Key Sectors

### H3: Healthcare — Clinical AI, Diagnostics, Patient Safety

### H3: Financial Services — Fraud Detection, Credit Scoring, Model Risk

### H3: Public Sector — Citizen Services, Automated Decisions

### H3: Corporate & Enterprise — HR Screening, Operations, Analytics

---

## H2: How DPO Consulting Supports AI Compliance & Responsible AI Adoption

### H3: AI Governance Framework Design

### H3: AI Risk Classification & Compliance Gap Assessments

### H3: High-Risk AI System Documentation & Technical File Preparation

### H3: Policy Development, Monitoring & Post-Market Surveillance

### H3: DPIAs, SIAs & Data Governance Enhancements

### H3: Training & Awareness for AI Stakeholders

### H3: Support for Vendors and AI Supply Chain Governance

---

## H2: Conclusion — Embedding Compliance Into AI Transformation

---

## H2: FAQ

Mamba

### H3: Is AI compliance mandatory for all AI systems?

### H3: What counts as a high-risk AI system?

### H3: Does AI compliance only apply to the EU AI Act?

### H3: How do we audit AI models for compliance?

### H3: What documentation do regulators expect?

---

## H2: References

# Written Article

Mamba

# What Is AI Compliance And Why It Matters: Regulatory, Ethical and Operational Drivers for Businesses

**Meta title:** Why AI Compliance Matters: AI Governance and Regulatory Compliance
**Meta description:** Learn why AI compliance matters, how global AI regulations are evolving, and how to build an AI compliance framework covering the EU AI Act, GDPR, NIST AI RMF, ISO/IEC 42001 and vendor risk.
**Suggested slug:** why-ai-compliance-matters
**Primary keyword:** AI compliance
**Secondary keywords:** AI regulatory compliance, artificial intelligence compliance, AI compliance framework, AI governance framework, responsible AI, EU AI Act compliance, AI risk management, AI compliance standards, regulatory compliance AI

AI compliance is becoming a core business issue. Organisations are no longer asking whether they should use artificial intelligence. They are asking how to use it safely, lawfully and at scale.

AI is now embedded in recruitment, customer support, fraud detection, credit scoring, healthcare, marketing, legal operations, cybersecurity, public services and internal productivity tools. It is also increasingly built into third-party software, cloud platforms, enterprise SaaS products and general-purpose AI systems.

This creates a new compliance challenge. AI risk is not only technical. It can become legal risk, privacy risk, cybersecurity risk, discrimination risk, contractual risk, reputational risk and operational risk.

A mature AI compliance framework helps organisations answer a simple question: can we prove that our AI systems are lawful, controlled, secure, explainable where necessary, and aligned with our risk appetite?

## What is AI compliance?

AI compliance is the process of ensuring that artificial intelligence systems are designed, procured, deployed and monitored in accordance with applicable laws, standards, internal policies and ethical expectations.

It includes regulatory compliance, but it is broader than regulation alone. A serious AI compliance programme should cover legal qualification, risk classification, data governance, cybersecurity, human oversight, transparency, vendor management, documentation, monitoring and incident response.

This is why AI compliance should not be treated as a one-off legal review before launch. It should be embedded into product development, procurement, IT security, privacy governance, enterprise risk management and operational controls.

In practical terms, AI compliance means knowing where AI is used, what it does, who is affected, what data it processes, which laws apply, which controls are in place, and how the organisation can evidence those controls.

## Why AI compliance matters now

AI adoption is accelerating faster than governance. Many organisations already use AI through public generative AI tools, embedded software features, vendor APIs, analytics platforms, HR tools, customer support systems or internal automation projects. In many cases, the legal, security and compliance teams only discover these uses after deployment.

This creates a governance gap. AI systems may process personal data, generate inaccurate outputs, influence decisions, expose confidential information, reproduce bias, create intellectual property issues or operate in ways that users do not understand.

At the same time, regulators, customers, investors and public authorities are increasing scrutiny. Enterprise buyers increasingly ask vendors to explain their AI use, provide documentation, confirm compliance with the EU AI Act, describe training data controls, evidence cybersecurity measures, and disclose whether general-purpose AI models are involved.

In this environment, AI compliance is no longer only about avoiding fines. It is about maintaining market access, protecting trust and making AI adoption scalable.

## Global AI regulations are evolving quickly

The AI regulatory landscape is moving from principles to enforceable obligations. Different jurisdictions are taking different approaches, but several themes are becoming common: risk classification, transparency, accountability, human oversight, data governance, safety, cybersecurity and lifecycle monitoring.

### EU AI Act compliance

Mamba

The EU AI Act is the first comprehensive horizontal AI regulation. It introduces a risk-based framework that classifies AI systems into prohibited practices, high-risk systems, transparency-risk systems and minimal or no-risk systems.

Some obligations are already applicable. Prohibited AI practices and AI literacy obligations started to apply in February 2025. Rules for general-purpose AI models started to apply in August 2025. The broader AI Act framework applies progressively, with important obligations coming into force in 2026 and beyond.

For organisations, EU AI Act compliance starts with classification. A business must determine whether a tool is an AI system, what role it plays under the regulation, whether the system is prohibited, high-risk, subject to transparency obligations, or lower risk, and whether it relies on a general-purpose AI model.

The practical consequence is that AI compliance cannot begin with a policy. It begins with an AI inventory and a documented risk classification process.

## United States AI compliance

The United States does not currently have a single horizontal AI law comparable to the EU AI Act. The U.S. approach is more fragmented and sector-driven.

For federal agencies, AI governance is shaped by executive orders and OMB guidance. For private-sector organisations, AI compliance often depends on consumer protection enforcement, privacy law, discrimination law, employment law, financial services regulation, healthcare regulation, product liability, cybersecurity expectations and sector-specific guidance.

This means that U.S. AI compliance is not “unregulated”. It is distributed across multiple legal and enforcement channels. Organisations operating in the U.S. should therefore align AI governance with sector obligations, consumer protection expectations and recognised frameworks such as the NIST AI Risk Management Framework.

## UK AI governance

The UK has taken a pro-innovation and principles-based approach to AI regulation. Rather than adopting a single horizontal AI statute equivalent to the EU AI Act, the UK has relied heavily on existing regulators applying cross-sectoral principles within their respective remits.

For businesses, this means that UK AI compliance is highly contextual. The relevant expectations may depend on whether the AI system is used in financial services, employment, healthcare, online services, public services, data protection or consumer-facing products.

The UK's Data (Use and Access) Act 2025 also changes aspects of UK data protection law, including the framework for automated decision-making. Organisations using AI to make or support significant decisions about individuals should therefore assess not only AI-specific governance, but also UK GDPR and data protection obligations.

### International AI standards and frameworks

Even where laws differ, AI compliance standards are converging around common operational practices.

The OECD AI Principles, updated in 2024, provide an international baseline for trustworthy AI. UNESCO's Recommendation on the Ethics of Artificial Intelligence sets a global ethical reference point. The NIST AI Risk Management Framework gives organisations a practical structure to govern, map, measure and manage AI risks. ISO/IEC 42001 provides a management system standard for organisations developing or using AI systems, while ISO/IEC 23894 supports AI risk management.

These frameworks do not replace legal analysis. However, they help organisations operationalise AI governance in a repeatable way, especially across multiple jurisdictions.

## The business risks of poor AI compliance

AI failures rarely remain technical. They become business events.

A customer support chatbot that provides incorrect advice may create liability and reputational harm. A recruitment tool that ranks candidates unfairly may create discrimination exposure. A generative AI tool that leaks confidential information may become a cybersecurity and contractual issue. A model used in credit, insurance, healthcare or employment may trigger regulatory scrutiny if it cannot be explained or challenged.

The first risk is legal exposure. Under the EU AI Act, certain infringements can lead to significant administrative fines, including the highest penalties for prohibited AI practices. Where personal data is involved, GDPR and other privacy laws may also apply, including obligations around lawful basis, transparency, DPIAs, rights handling and data security.

The second risk is reputational damage. Stakeholders increasingly interpret AI failure as governance failure. If an organisation deploys AI that is discriminatory, unsafe, misleading or uncontrolled, the issue is rarely seen as a model problem. It is seen as a leadership and accountability problem.

The third risk is operational instability. AI systems can drift, hallucinate, overfit, amplify biased data, change behaviour after vendor updates, or produce outputs that users

over-rely on. Without monitoring and clear escalation rules, these issues may scale before anyone detects them.

The fourth risk is vendor dependency. Many organisations do not build AI systems internally. They buy AI through SaaS platforms, APIs or embedded product features. If vendor documentation is weak, training data is opaque, model changes are unannounced or contractual protections are insufficient, third-party AI risk becomes internal risk.

## AI compliance as a competitive advantage

AI compliance is often presented as a constraint. In reality, it can become a competitive advantage.

Enterprise customers increasingly want proof that AI is governed. They ask where AI is used, which models are involved, whether personal data is processed, whether outputs are reviewed, whether human oversight exists, whether the vendor can support regulatory obligations, and whether AI-generated content is disclosed.

An organisation that can answer these questions clearly will move faster in procurement, reduce friction in due diligence and build trust with customers, regulators and partners.

Good AI compliance also accelerates internal adoption. Employees are more likely to use AI confidently when they know which tools are approved, which data can be entered, which use cases require review, and when human validation is mandatory.

This is the real purpose of an AI compliance framework: not to block AI, but to make AI deployment defensible, repeatable and scalable.

## Core components of an AI compliance framework

A mature AI compliance framework should cover both AI systems developed internally and AI systems purchased or embedded through vendors. It should also cover general-purpose AI tools used by employees, product teams or customer-facing functions.

### AI inventory and risk classification

The foundation of AI compliance is an AI inventory. Organisations need a clear record of where AI is used, by whom, for what purpose, with which data, through which vendor or model, and with what potential impact.

The inventory should not be limited to formal data science projects. It should include generative AI tools, vendor AI features, HR tools, customer service automation, analytics models, embedded AI in SaaS products, cybersecurity tools, productivity assistants and experimental pilots.

Once inventoried, each system should be classified. For EU AI Act compliance, this means assessing whether the system is prohibited, high-risk, subject to transparency obligations, linked to a general-purpose AI model, or minimal risk. For broader AI compliance, the organisation should also assess privacy, security, ethical, contractual, operational and reputational risk.

## Data governance

AI governance depends on data governance. If the organisation cannot explain where data came from, whether it was lawfully collected, whether it can be reused, whether it contains personal or sensitive data, and whether it is accurate and representative, the AI compliance position will be weak.

Data governance should cover data provenance, lawful basis, permissions, minimisation, quality, representativeness, bias, retention, deletion, access control and documentation. This is especially important when data is used to train, fine-tune or evaluate AI models.

For AI systems processing personal data, privacy compliance and AI compliance must be connected. “We already had the data” is not enough to justify a new AI use case.

## Transparency and explainability

Transparency is both a legal obligation and a trust requirement. Under the EU AI Act, certain systems must inform people that they are interacting with AI, and certain AI-generated or manipulated content must be disclosed. Under privacy laws, organisations may need to explain how personal data is used, especially when AI affects individuals.

Explainability should be understood practically. Not every AI system needs to disclose full model architecture. But organisations should be able to explain the system’s purpose, its intended use, its main limitations, the type of inputs it relies on, the role of human review, and how affected individuals can raise concerns where relevant.

For high-impact use cases, explainability is also an operational control. If users cannot understand the limits of an AI system, they may over-rely on its outputs.

## Human oversight

Human oversight is central to responsible AI and to many regulatory frameworks. But it must be meaningful.

A vague statement that “a human remains in the loop” is not enough. The organisation should define who reviews AI outputs, when intervention is required, what information the reviewer receives, whether the reviewer has authority to override the AI, and how decisions are documented.

This is particularly important where AI affects employment, credit, healthcare, education, access to services, public-sector decisions or other consequential outcomes.

## Cybersecurity and technical controls

AI introduces specific security risks. These may include prompt injection, data poisoning, model inversion, model extraction, sensitive data leakage, unauthorised fine-tuning, insecure APIs, supply chain compromise and adversarial attacks.

An AI compliance framework should therefore include cybersecurity controls adapted to AI systems. This may involve secure development practices, access control, secrets management, model endpoint protection, red teaming, adversarial testing, monitoring, incident response and vendor security review.

Cybersecurity should not be treated as an annex to AI governance. It is one of its core components.

## Monitoring and lifecycle management

AI systems change over time. Data changes, users change, vendor models change, performance changes and risks evolve. A compliance assessment performed before deployment will not be sufficient if the system is not monitored.

Organisations should define how AI systems are reviewed after deployment. Monitoring may include performance metrics, drift detection, bias indicators, error rates, user complaints, incident logs, override rates, vendor update reviews and periodic reassessment.

For higher-risk systems, monitoring should be formalised and documented. For lower-risk systems, lighter review may be sufficient. The key is proportionality.

## Documentation and audit readiness

AI compliance must be evidenced. Regulators, customers, auditors, investors and litigants may ask how the organisation classified a system, what data it used, what risks were identified, what controls were implemented and how the system is monitored.

Documentation may include the AI inventory, risk classification records, DPIAs, fundamental rights assessments, technical documentation, model cards, vendor due diligence, policies, training records, monitoring reports, incident records and approval decisions.

Documentation is not bureaucracy when it helps the organisation prove control.

## AI compliance and data protection

AI compliance and data protection are deeply connected. Many AI systems process personal data during training, fine-tuning, inference, evaluation or monitoring. This means that GDPR, UK GDPR and other privacy laws may apply alongside AI-specific regulation.

The first issue is lawful basis. Organisations must identify a valid lawful basis for processing personal data. If special category data is involved, additional conditions apply. Reusing existing data for AI training or analytics may require a fresh assessment of purpose limitation and compatibility.

The second issue is transparency. Individuals should understand how their data is used, especially where AI supports decisions affecting them.

The third issue is DPIA. AI systems involving profiling, large-scale data processing, sensitive data, vulnerable individuals or significant effects on individuals will often require a data protection impact assessment.

The fourth issue is individual rights. AI does not remove access, objection, rectification or transparency obligations. Where solely automated decisions produce legal or similarly significant effects, additional safeguards may apply, including human intervention and the ability to contest the decision in relevant circumstances.

A privacy-by-design approach is therefore essential for AI compliance.

## AI compliance across key sectors

AI compliance priorities differ by sector.

In healthcare, AI may affect diagnosis, triage, treatment recommendations, patient monitoring or clinical operations. The key concerns are patient safety, validation, sensitive data, clinical accountability, medical device qualification and monitoring.

In financial services, AI may be used for fraud detection, credit scoring, risk modelling, customer segmentation, insurance pricing, anti-money laundering or investment support.

The main issues are fairness, explainability, auditability, model risk management, consumer protection and regulatory accountability.

In employment, AI may be used to screen CVs, rank candidates, evaluate performance, monitor productivity or support disciplinary decisions. These uses are sensitive because they affect livelihoods and may create discrimination or employee privacy risks.

In the public sector, AI can affect access to benefits, citizen services, inspections, enforcement or resource allocation. Transparency, accountability, human oversight and fundamental rights impact assessment are essential.

In corporate environments, generative AI may be used for drafting, summarisation, research, coding, customer communications or internal productivity. The risks include confidentiality, hallucination, intellectual property, data leakage, over-reliance and lack of auditability.

A single AI compliance policy will not be enough for all of these contexts. Organisations need a risk-based operating model.

## How to build an AI compliance strategy

An effective AI compliance strategy should start with visibility. The organisation should identify AI systems already in use, AI systems being developed, vendor tools with AI features and public AI tools used by employees.

The next step is classification. Each system should be assessed based on its purpose, users, affected persons, data, level of automation, human oversight, jurisdictional exposure and potential impact. For EU-facing systems, the classification should be mapped against the AI Act.

The organisation should then perform a gap assessment. This means comparing the current state with applicable requirements: EU AI Act, GDPR, UK GDPR, sector rules, contractual obligations, cybersecurity standards and internal policies.

Governance should then be defined. The organisation needs clear roles: AI system owner, legal owner, privacy owner, security owner, procurement owner, risk owner and business approver. It also needs clear review gates before pilot, production deployment and major changes.

For higher-risk systems, the organisation should conduct DPIAs, fundamental rights assessments, model risk assessments or broader impact assessments. These assessments should not remain theoretical. They should produce concrete mitigations, acceptance criteria and go/no-go decisions.

Monitoring should then be embedded into operations. AI systems should be reviewed periodically, with frequency depending on risk. Vendor systems should be reassessed when models, terms, data practices or functionalities change.

Finally, teams must be trained. AI literacy is not only a regulatory expectation under the EU AI Act. It is also a practical control against shadow AI, poor prompting, data leakage, over-reliance and misuse.

## How DPO Consulting supports AI compliance

DPO Consulting supports organisations in building AI compliance programmes that are legally sound, operationally practical and aligned with business objectives.

Our support can include AI inventory design, AI system classification, EU AI Act readiness, GDPR alignment, DPIAs, fundamental rights impact assessments, AI governance framework design, AI policy drafting, vendor due diligence, contract review, technical documentation support, AI literacy training and monitoring processes.

We also help organisations align their AI compliance framework with recognised standards and frameworks such as ISO/IEC 42001, ISO/IEC 23894 and the NIST AI Risk Management Framework.

Our approach is pragmatic. We do not treat AI compliance as a standalone legal exercise. We connect legal obligations with product development, procurement, cybersecurity, data governance, risk management and operational controls.

The objective is to help organisations deploy AI responsibly, reduce regulatory exposure, satisfy customer and investor scrutiny, and create a governance model that can scale.

## Conclusion: AI compliance is becoming a core capability

AI compliance is no longer optional for organisations that want to deploy artificial intelligence at scale. The regulatory landscape is evolving, but the operational direction is already clear: organisations must know where AI is used, classify risks, document decisions, control data, manage vendors, train teams, monitor systems and maintain evidence.

The companies that succeed will not be those that wait for every law to become fully enforceable. They will be those that build AI governance into the way they operate.

AI compliance should therefore be seen as a business enabler. It helps organisations innovate with confidence, earn trust, satisfy procurement expectations and reduce the risk that AI adoption turns into legal, operational or reputational failure.

# FAQ

## What is AI compliance?

AI compliance is the process of ensuring that AI systems are developed, procured, deployed and monitored in accordance with applicable laws, standards, policies and risk controls. It covers legal compliance, data protection, cybersecurity, transparency, human oversight, documentation and monitoring.

## Is AI compliance mandatory?

AI compliance is mandatory where specific laws apply, such as the EU AI Act, GDPR, sector regulations or consumer protection rules. Even where no AI-specific law applies, organisations should still implement governance controls to manage legal, security, ethical and operational risk.

## What is an AI compliance framework?

An AI compliance framework is a structured operating model for governing AI. It usually includes an AI inventory, risk classification, data governance, transparency rules, human oversight, cybersecurity controls, vendor management, monitoring, documentation and training.

## How does the EU AI Act affect AI compliance?

The EU AI Act requires organisations to classify AI systems by risk level. It prohibits certain AI practices, imposes strict obligations on high-risk AI systems, creates rules for general-purpose AI models and introduces transparency obligations for certain AI systems and AI-generated content.

## Does AI compliance only concern high-risk AI?

No. High-risk AI systems require the most extensive controls, but lower-risk AI systems may still trigger transparency, privacy, cybersecurity, contractual, employment or consumer protection obligations. AI literacy and governance are also relevant beyond high-risk systems.

## How does GDPR apply to AI?

Mamba

GDPR applies when AI systems process personal data. Organisations must identify a lawful basis, provide transparency, respect purpose limitation and data minimisation, implement security measures, support individual rights and conduct DPIAs where processing is likely to result in high risk.

## What are the main AI compliance standards?

Common AI compliance standards and frameworks include ISO/IEC 42001 for AI management systems, ISO/IEC 23894 for AI risk management, the NIST AI Risk Management Framework, OECD AI Principles and UNESCO's Recommendation on the Ethics of Artificial Intelligence.

## How can organisations start an AI compliance programme?

The best starting point is an AI inventory. Organisations should identify where AI is used, classify systems by risk, assess applicable laws, review vendors, define governance roles, train teams and document decisions.

## What is shadow AI?

Shadow AI refers to the use of AI tools without organisational approval or oversight. It often occurs when employees use public generative AI tools, unapproved APIs or AI features embedded in software without legal, privacy or security review.

## How can DPO Consulting help with AI compliance?

DPO Consulting helps organisations design and implement AI compliance programmes, including AI inventories, EU AI Act classification, GDPR alignment, DPIAs, AI governance frameworks, vendor assessments, policies, documentation and AI literacy training.

# 📚 Content Guidelines

Mamba

# Content Writing Guidelines

👉 Live document

**Table of Contents**



*All content delivered to clients must follow the guidelines listed in this document.

Writer Responsibility: It is the responsibility of each writer to ensure the accuracy and clarity of their content. Content outlines serve as a starting point. Writers are expected to assess the flow, fix headings, reduce redundancies, verify all claims with credible sources, and ensure that internal links and anchors accurately support the text.