sonatype

Guide to

AI regulations

in software development

Artificial Intelligence (AI) is **transforming software development**, enabling faster coding, improved decision-making, and automated processes.

However, as AI becomes more integrated into critical infrastructure, concerns over security, privacy, fairness, and accountability have prompted governments worldwide to introduce laws on artificial intelligence. Organizations need to **prepare for these regulations to ensure compliance**, mitigate risks, and build trust in their **AI-powered software solutions**.

AI regulations and frameworks largely focus on similar key principles — **ethics, transparency, and security**. While some regulations are still in development, governing bodies globally continue to align on the necessity of AI governance. When such alignment occurs, it signals significant financial investment, competition, and regulatory scrutiny.

International AI regulations and guidelines

As artificial intelligence continues to evolve, international organizations and governing bodies are actively working to establish regulatory frameworks that ensure AI is used responsibly.

Many of these frameworks share common themes, such as promoting ethical AI development, safeguarding human rights, and increasing transparency in AI-driven decision-making. While some of these initiatives are still in their early stages, they provide a glimpse into how AI governance will take shape globally.

Below are key international AI regulations and guidelines that organizations should be aware of as they prepare for compliance in an increasingly regulated landscape.

European Union AI Act

The **European Union (EU) AI Act** is one of the most comprehensive regulatory efforts to date, modeled after the **General Data Protection Regulation (GDPR)**.

As a proposed EU AI regulation, the act categorizes AI applications into risk levels:

- **Unacceptable risk** (e.g., social scoring systems) – Banned.
- **High risk** (e.g., biometric identification, critical infrastructure AI) – Subject to strict compliance requirements.
- **Limited risk** (e.g., AI chatbots) – Requires transparency disclosures.
- **Minimal risk** (e.g., AI-powered spam filters) – Minimal regulation.

The regulation emphasizes human oversight, data governance, data governance, and cybersecurity for high-risk AI systems. Organizations deploying such systems will be required to perform risk assessments, maintain detailed documentation, and register their models with an EU-wide database.

This proposed EU AI Act is part of a broader wave of digital regulations, including the **Cyber Resilience Act (CRA)**, which introduces new requirements for software security and supply chain transparency. Together, these efforts signal a coordinated regulatory push within the EU to make digital systems — including AI — more trustworthy and resilient.

OECD AI principles

The Organisation for Economic Co-operation and Development (OECD) **established AI principles** promoting fairness, security, and human rights.

These five principles — originally adopted by over 40 countries — encourage the development of AI that is:

- Inclusive and human-centered
- Transparent and explainable
- Robust, secure, and safe throughout its lifecycle
- Accountable to individuals and society
- Consistent with democratic values and the rule of law

While not legally binding, these principles serve as an influential foundation for national AI policies and have helped shape several emerging regulatory AI frameworks worldwide, including those within the EU and North America.

UNESCO AI ethics framework

The United Nations Educational, Scientific and Cultural Organization (UNESCO) has **developed a comprehensive set of ethical guidelines for AI**, adopted by all 193 member states.

This framework promotes the development and deployment of AI in ways that uphold:

- Human rights and dignity
- Privacy protection and data governance
- Fairness, inclusivity, and non-discrimination
- Environmental responsibility and sustainability

UNESCO's AI ethics framework also emphasizes the importance of international cooperation, capacity-building in developing countries, and gender equality in AI development. It is one of the most globally unified ethical visions for AI and is intended to guide national governments as they craft enforceable AI policies.

Country-specific AI regulations

United States AI regulatory landscape

The United States does not currently have a comprehensive federal AI law, but regulatory momentum is building across federal agencies and state governments.

Rather than pursue a single sweeping regulation, the U.S. is taking a sector-specific and agency-driven approach to AI governance, emphasizing innovation while addressing risks related to fairness, transparency, and accountability.

Key initiatives include:

- **NIST AI Risk Management Framework (AI RMF):** Developed by the National Institute of Standards and Technology (NIST), **this voluntary framework** provides guidance for managing risks associated with the design, development, deployment, and use of AI systems. The framework promotes principles such as trustworthiness, safety, security, privacy, and fairness, and is designed to be adaptable across sectors.
- **Executive Orders and Federal Agency Policies:** While previous executive orders on AI governance were rescinded or replaced, the current administration has expressed strong support for responsible AI through agency-specific guidelines. This includes AI policies issued by the Office of Management and Budget (OMB) and the White House Office of Science and Technology Policy (OSTP).
- **California Consumer Privacy Act (CCPA):** While not specific to AI, the CCPA — and its expansion under the California Privacy Rights Act (CPRA) — has significant implications for AI systems that rely on personal data. These laws introduce individual rights over automated decision-making and could inform future AI legislation in the U.S.

Several other states, such as Illinois, Virginia, and Colorado, are also exploring AI legislation or expanding privacy laws that intersect with AI usage. As discussions around a federal AI framework continue, companies operating in the U.S. must navigate a complex regulatory landscape.

China's AI regulations

China has **enacted AI policies** prioritizing national security, public safety, and data governance. These regulations aim to exert strong governmental control over the development and deployment of AI, ensuring alignment with national priorities.

Key regulations include:

- **Deep synthesis provisions** aim to combat misinformation and deepfakes. These provisions require transparency, labeling, and consent for AI-generated content. Service providers must also implement data security protections and submit security assessments for sensitive AI systems.
- **Shenzhen AI regulations** serve as regional initiatives to boost AI innovation in one of China's major tech hubs. These rules encourage responsible AI development and explicitly prohibit systems that promote discrimination or violate privacy rights.

Several other states, such as Illinois, Virginia, and Colorado, are also exploring AI legislation or expanding privacy laws that intersect with AI usage. As discussions around a federal AI framework continue, companies operating in the U.S. must navigate a complex regulatory landscape.

Canada's Artificial Intelligence and Data Act (AIDA)

Canada's **AIDA**, part of the broader **Bill C-27**, is among the most advanced national legislative proposals addressing AI. It seeks to regulate AI systems based on their potential impact on individuals and society.

AIDA would:

- Introduce a risk-based framework for classifying AI systems.
- Mandate transparency and accountability for high-impact AI systems, such as those affecting healthcare, employment, and financial services.
- Establish enforcement mechanisms, including potential audits and financial penalties, for organizations that violate this AI law.

f enacted, AIDA would create new obligations for businesses deploying AI and require them to ensure safety, explainability, and fairness in their systems.

Australia's AI Ethics Framework

Australia's approach to AI regulation is currently **principles-based** rather than prescriptive. The country has issued a set of eight non-binding AI ethics principles designed to guide both private and public sector organizations.

These principles emphasize:

- Human-centered values and fairness
- Transparency and explainability in AI systems
- Robustness and security to ensure systems operate safely
- Accountability for decisions made using AI

While not yet enforceable as law, these principles lay the groundwork for future AI legislation and provide a framework for ethical AI innovation.

United Kingdom's National AI Strategy

The **UK AI Strategy** is a 10-year plan to position the UK as a global leader in the development and deployment of artificial intelligence. While distinct from the broader EU AI regulation efforts, it aligns in many areas, including **ethics, security, and innovation**.

This strategy is rooted in three core pillars:

- **Investing in the long-term needs of the AI ecosystem,** including skills development, research funding, and public-private partnerships.
- **Supporting the transition to an AI-enabled economy,** encouraging adoption across industries and providing tools for responsible AI integration.
- **Governing AI effectively** through a pro-innovation regulatory environment that balances safety, transparency, and flexibility.

In 2023, the UK government published an AI white paper outlining its intent to implement a light-touch, sector-specific regulatory approach, with regulators expected to adapt guidance based on the context in which AI is used. This flexible model is designed to encourage innovation while still addressing risks, and it includes commitments to develop technical standards and foster public trust.

The role of SBOMs in AI governance

As the AI regulatory landscape evolves, organizations must ensure visibility and compliance with AI components in their software supply chains. This is where a **software bill of materials (SBOM)** comes into play.

An SBOM is a detailed inventory of software components, including open source libraries and AI models. It gives organizations the ability to track **dependencies** across their software, identify **vulnerabilities** before they become liabilities, ensure compliance with regulatory and licensing requirements, and improve transparency into the AI models they use or distribute.

Sonatype solutions for AI compliance and governance

Sonatype's approach to AI compliance is rooted in helping organizations build and maintain trustworthy AI-enabled software by addressing the core risks outlined in emerging AI regulations and security frameworks.

Sonatype Repository Firewall allows customers to block the most dangerous models from ever entering their repository. With Sonatype SBOM Manager and Sonatype Lifecycle, customers gain the tools they need to document, monitor, and manage AI model risk across the software supply chain. Shifting AI model decisions away from runtime helps organizations evaluate risk before it can be exploited in production.

Model risk mitigation

Sonatype SBOM Manager enables users to evaluate AI and ML model components for known vulnerabilities, license risks, and even malware threats, especially in open source packages or third-party dependencies.

With Sonatype Lifecycle, these evaluations can be integrated directly into CI/CD pipelines, ensuring that high risk models are flagged and blocked early in development.

Record keeping and traceability

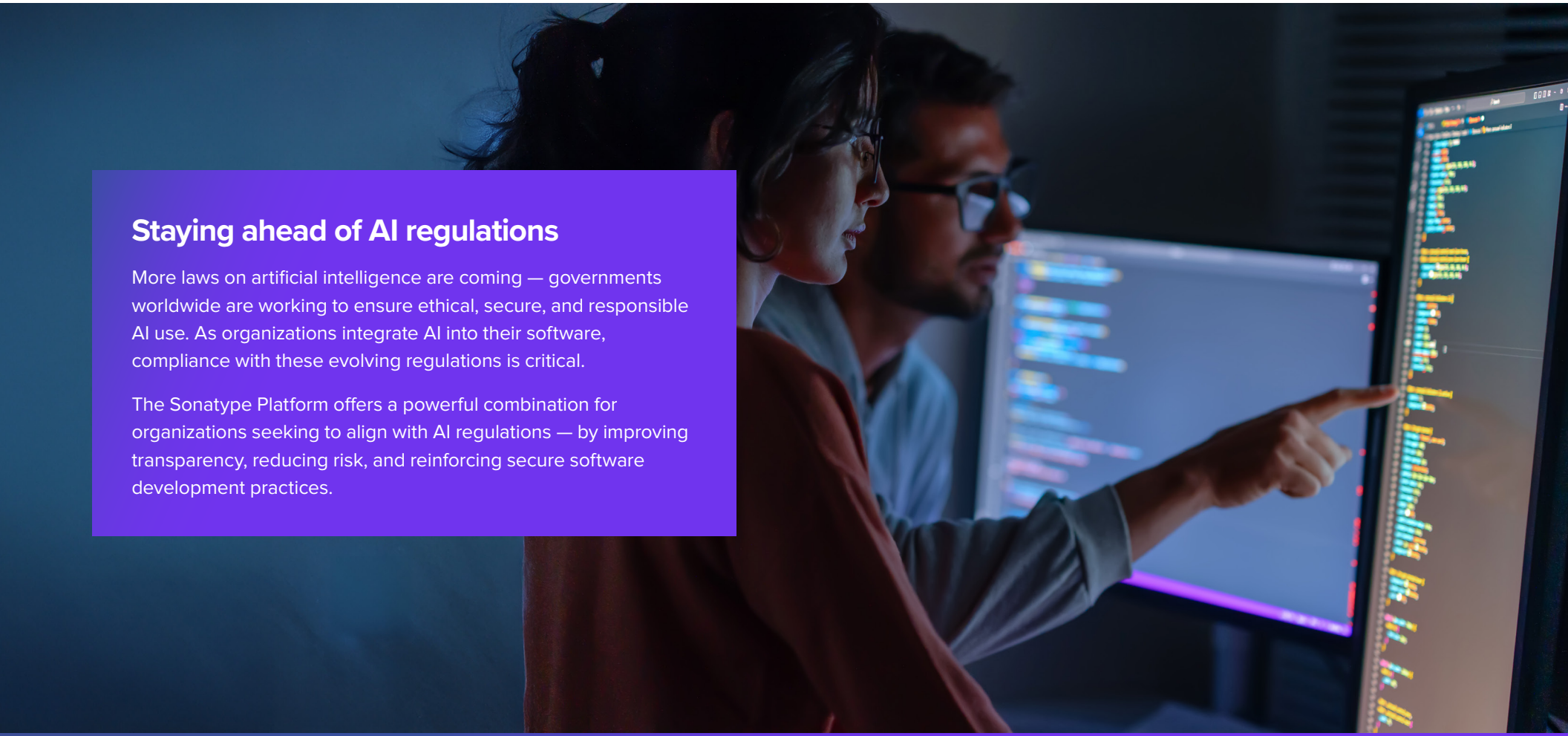
Regulatory requirements often demand full transparency of how AI models are sourced, trained, and updated. Sonatype SBOM Manager and Sonatype Lifecycle supports detailed record keeping of the exact model and its metadata.

Although it does not expose training datasets, organizations can still document and share contextual metadata for traceability and governance purposes, especially valuable when paired with internal audit practices.

Sonatype Lifecycle builds on this with policy enforcement and historical auditing capabilities across development stages.

Bias and content controls

While Sonatype does not assess model outputs directly, organizations can define custom policies in Sonatype Lifecycle to flag packages or models that have known content-related risks or come with warnings of inappropriate or biased usage. This supports compliance with ethical AI principles such as fairness and non-discrimination.



Staying ahead of AI regulations

More laws on artificial intelligence are coming — governments worldwide are working to ensure ethical, secure, and responsible AI use. As organizations integrate AI into their software, compliance with these evolving regulations is critical.

The Sonatype Platform offers a powerful combination for organizations seeking to align with AI regulations — by improving transparency, reducing risk, and reinforcing secure software development practices.

sonatype

Sonatype is the software supply chain security company. We provide the world's best end-to-end software supply chain security solution, combining the only proactive protection against malicious open source, the only enterprise grade SBOM management and the leading open source dependency management platform. This empowers enterprises to create and maintain secure, quality, and innovative software at scale. As founders of Nexus Repository and stewards of Maven Central, the world's largest repository of Java open-source software, we are software pioneers and our open source expertise is unmatched. We empower innovation with an unparalleled commitment to build faster, safer software and harness AI and data intelligence to mitigate risk, maximize efficiencies, and drive powerful software development. More than 2,000 organizations, including 70% of the Fortune 100 and 15 million software developers, rely on Sonatype to optimize their software supply chains. To learn more about Sonatype, please visit www.sonatype.com.

Headquarters
8161 Maple Lawn Blvd,
Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High
St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
60 Martin Place,
Level 1
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com