KPMG

Embedding privacy across the AI lifecycle: from principles to practice

2026

KPMG International | kpmg.com

KPMG. Make the Difference.

Executive summary

Every technological breakthrough brings new opportunities and new questions.

Artificial Intelligence (AI) not only transforms how the world works, make decisions, and interact; it also redefines our collective understanding of ethics, privacy, and trust in the digital age.

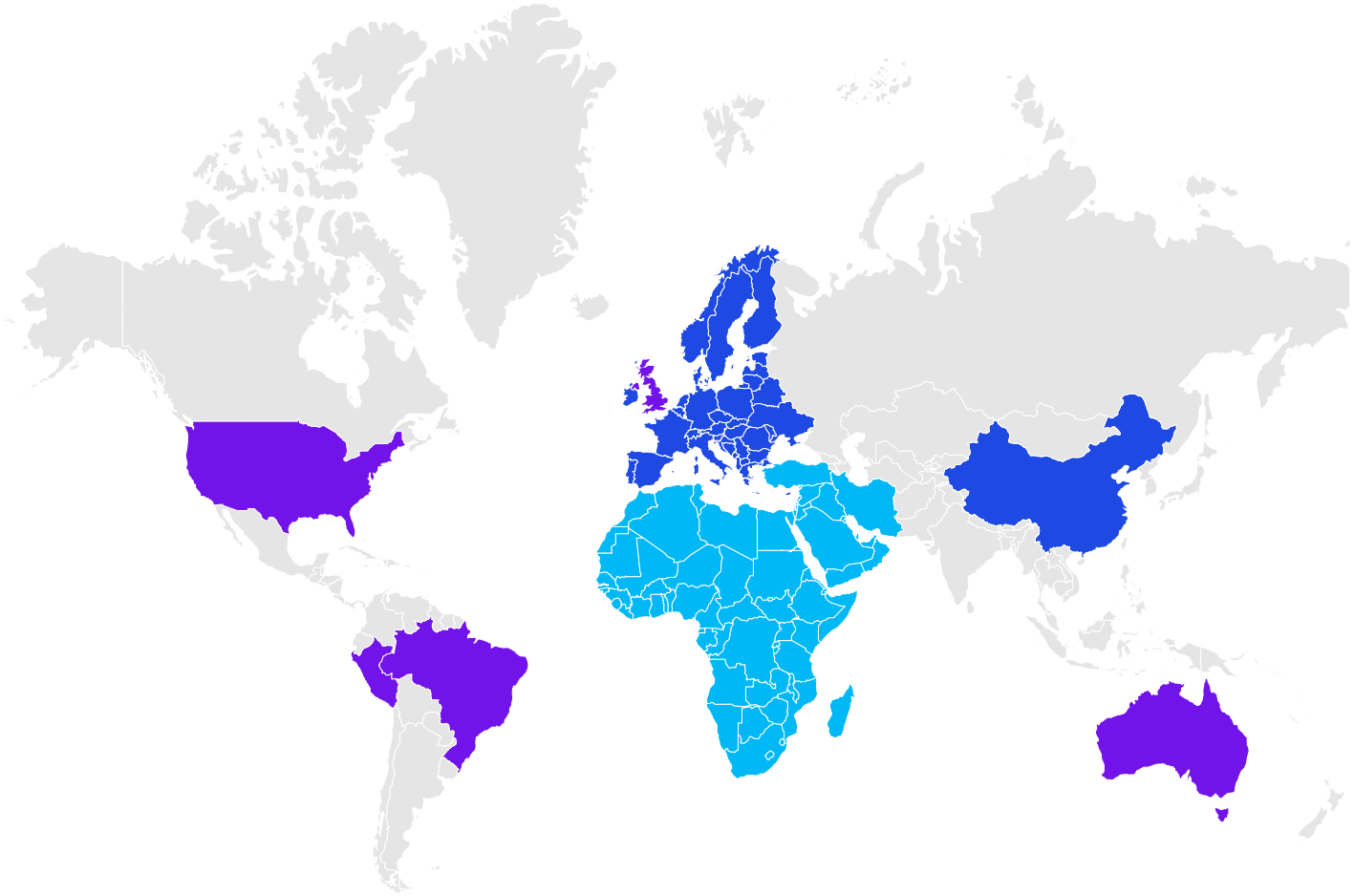
This paper explores **how privacy, long recognized as a core value, has emerged as a foundational pillar in AI governance**. The protection of personal data can no longer be treated as an ancillary requirement; it **should be embedded** as a structural principle **throughout all phases of the AI lifecycle**: from design and training to deployment, oversight, continuous improvement and decommissioning.

Privacy embedded across the AI lifestyle

Executive summary

The **global landscape** of AI governance remains fragmented, with both international and regional developments shaping the field. At the global level, organizations such as the G7, the Council of Europe, the UN[1] and its agencies, and the OECD[2] have advanced principles that emphasize transparency, accountability, and human rights. **Regionally**, diverse approaches are emerging in the **United States**, the regulatory landscape is shaped by state-level legislation and by the federal Administration, including recent Executive Orders from the White House[3], as well as the Federal Trade Commission (FTC)[4], which plays a central role in promoting principles of transparency, security, and accountability. In **Asia-Pacific**, models range from China's stringent regulations to Japan and **Australia's** voluntary frameworks. **Latin America**, the **Middle East**, and **Africa** are beginning to establish their own frameworks, often using data protection as an entry point into broader digital privacy and AI governance.

Europe is among the leading jurisdictions with binding instruments such as the GDPR and the AI Act. Together, they integrate data protection requirements with broader privacy safeguards and explicitly address issues such as risk management, automated decision-making, and profiling. This reflects a wider global recognition that AI-related privacy challenges go beyond the protection of personal data to include fairness, bias, model drift, and systemic impacts.



Executive summary

Despite regional differences, both technological progress and geopolitical considerations underscore the need for enhanced international cooperation, not only to foster innovation and economic growth, but also to safeguard fundamental rights, including privacy, and **to build trust as the cornerstone of ethical and sustainable AI**.

At KPMG, we believe that well-designed regulation supports organizations in leveraging AI systems in a trusted and privacy-respecting manner. A robust regulatory framework can act as a catalyst for trust, protects individuals, and helps to ensure that AI is deployed under a **Trusted AI approach**. This means developing AI that is reliable, ethical, and sustainable, where privacy is not limited to the design or deployment phase, but is embedded throughout the AI system's lifecycle; aligning technological advancement with fundamental rights.

In this document, **KPMG specialists seek to examine how different regions are approaching privacy and AI governance**, outlining the regulatory, ethical, and geopolitical frameworks that are shaping this landscape, as well as the challenges and opportunities they create. We also **highlight how KPMG's Trusted AI approach helps organizations in embedding privacy and fundamental rights as core principles across the AI lifecycle**, from design and training to deployment, oversight, and decommissioning; with the aim of building a balanced approach to innovation, accountability, resilience, and trust.

Index

Global landscape of privacy and Artificial Intelligence

Global landscape of privacy and Artificial Intelligence

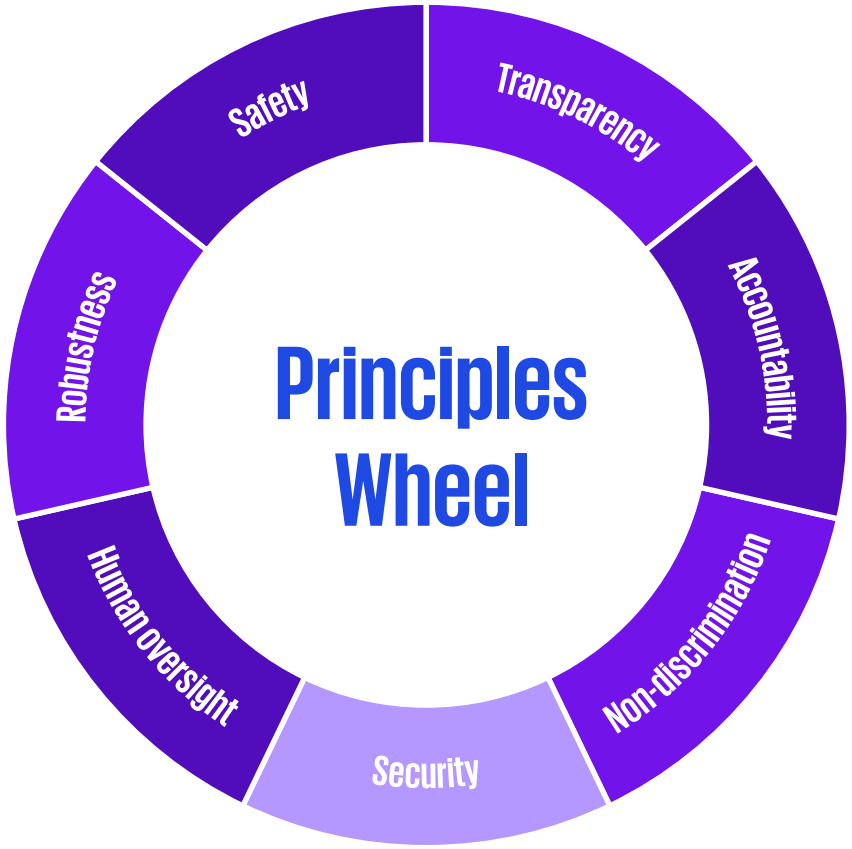
Artificial Intelligence and privacy: A global governance overview

Artificial Intelligence (AI) increasingly relies on vast volumes of data for training, much of which is personal data. This reality underscores the need to align privacy regulations and preferred practices with AI development, with the aim of ensuring that innovation progresses without compromising individual rights. At the same time, it is essential to implement effective security measures for data storage and processing, which seek to limit exposure risks and preserving public trust.

As AI becomes more embedded in our lives, a global convergence is emerging around key principles such as **transparency**, **accountability**, **non-discrimination**, and **security** which are aligned with the OECD's 2019 Principles for Trustworthy AI[2]. These principles emphasize the importance of **robustness**, **safety**, and **human oversight** throughout the AI lifecycle.

However, the pace and intensity with which these principles are translated into regulation vary significantly, resulting in a fragmented landscape: while some regions advance with binding frameworks, others rely on ethical guidelines or sector-specific initiatives.

International bodies, such the United Nations High Commissioner for Human Rights[6], have promoted similar principles, emphasizing dignity, autonomy, and accountability. This reflects a global convergence toward a shared standard, with Europe positioned as a regulatory leader aligned with internationally recognized frameworks and principles.



Global landscape of privacy and Artificial Intelligence

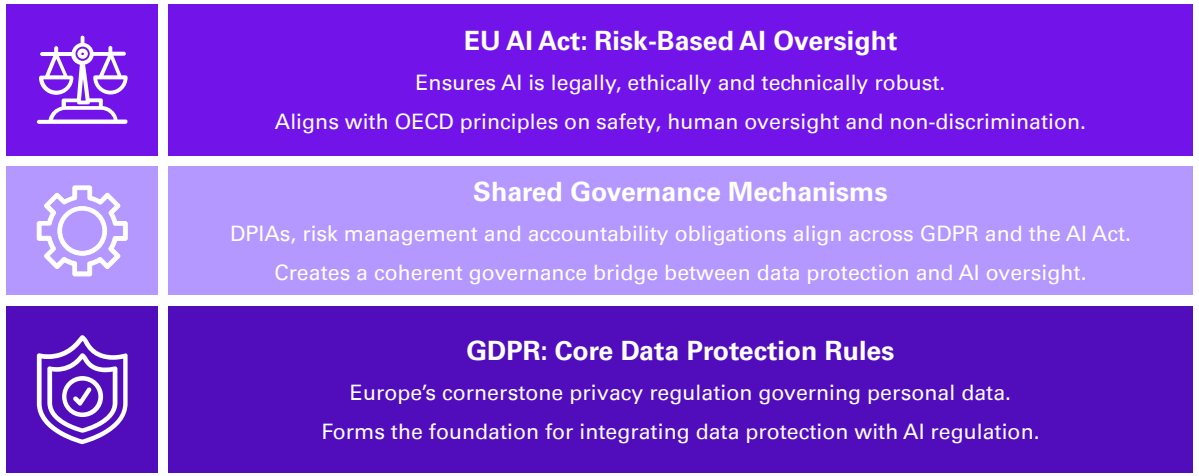
Artificial Intelligence and privacy: A global governance overview

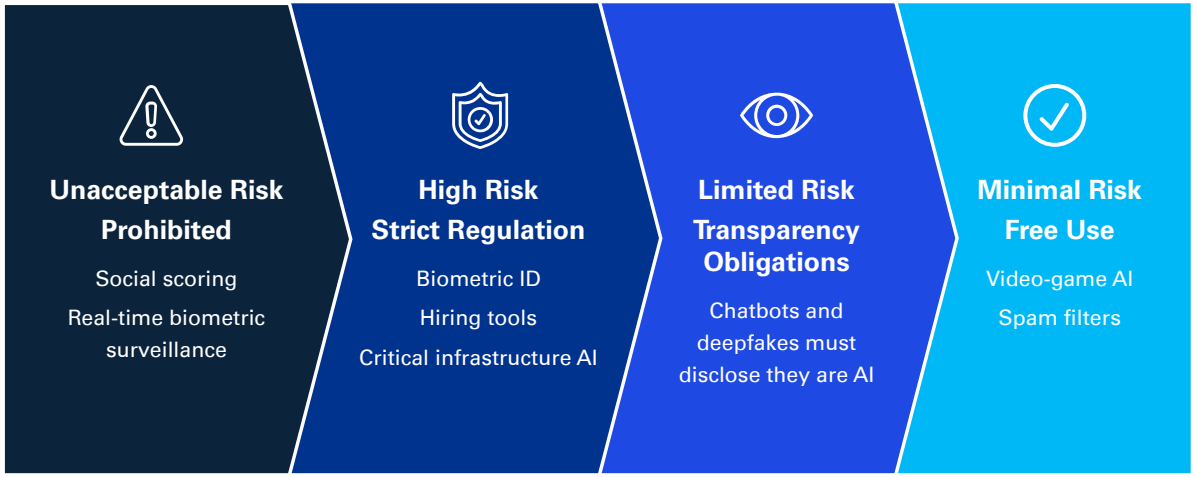
Europe has emerged as a regulatory benchmark adopted in 2024, introduces a risk-based framework that classifies AI systems and imposes specific requirements for those deemed "high-risk", such as biometric identification, employment processes, or critical infrastructure management. The regulation reinforces OECD principles by mandating that AI systems should be legally, ethically, and technically robust, and that they uphold democratic values, human rights, and the rule of law.

In parallel, the GDPR remains the cornerstone of privacy regulation in Europe. Building on this foundation, the European Union's AI Act reinforces and expands obligations such as impact assessments, risk management, and the principle of "Privacy by Design" (from now onwards also PbD). Together, these instruments establish the EU as one of the most advanced jurisdictions in coherently integrating data protection and AI regulation.

This convergence between the GDPR and the AI Act has been highlighted in recent analyses, which emphasize how both frameworks complement each other by aligning data protection obligations with AI risk-based governance requirements. As noted by Compact Journal (2024)[8], GDPR compliance processes such as data protection impact assessments and accountability mechanisms can serve as a foundation for meeting key obligations under the AI Act, bridging the two regimes and promoting consistent, trustworthy AI practices across the EU.

Other Europeans jurisdictions, such as the United Kingdom and Switzerland, are also progressing with their own frameworks, adding to the region's regulatory momentum.





Global landscape of privacy and Artificial Intelligence

Belgian Data Protection Authority Perspective: GDPR obligations across the AI lifecycle

The Belgian Data Protection Authority (DPA) has published guidance clarifying how the GDPR applies to artificial intelligence systems and how these obligations interact with the EU Artificial Intelligence Act. The information brochure emphasizes that AI does not operate outside existing data protection law and that the GDPR remains fully applicable to AI systems processing personal data.

Rather than introducing new concepts, the Belgian DPA frames AI regulation as a **continuation and operationalization of GDPR principles** across the AI lifecycle. The guidance highlights the close relationship between the GDPR and the AI Act, positioning them as complementary frameworks that jointly govern the design, deployment and use of AI systems in Europe.

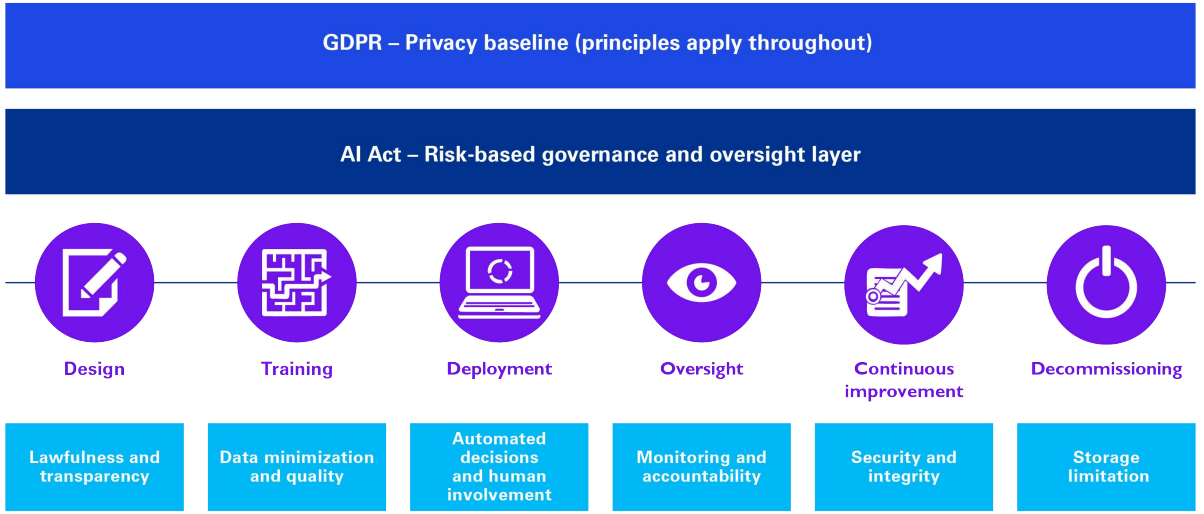
The Belgian DPA adopts a **lifecycle-based approach**, emphasizing that data protection obligations apply from the earliest stages of AI system design and training through deployment, monitoring and decommissioning. Compliance is expected to be addressed throughout AI development and operation, rather than only at the point of use.

Coherent integration of GDPR and AI Act obligations

This convergence between the GDPR and the AI Act is reflected in the Belgian DPA's emphasis on accountability, risk management and documentation. Existing GDPR governance tools, such as data protection impact assessments, records of processing activities and transparency documentation, are presented as essential building blocks for AI governance. For high-risk AI systems, the Belgian DPA highlights that GDPR requirements (including DPIAs and safeguards for automated decision-making) and AI Act obligations (such as risk classification, human oversight and fundamental rights impact assessments) should be aligned and mutually reinforcing, rather than treated as separate compliance exercises.

Supervisory signal

The Belgian DPA positions GDPR compliance not as a legacy obligation, but as a structural enabler of trustworthy and lawful AI. Organizations that have embedded privacy-by-design, accountability and risk management under the GDPR are better placed to meet the requirements of the AI Act and to deploy AI systems in a responsible and sustainable manner.



In the broader European context, the Belgian DPA's guidance illustrates how supervisory authorities are moving from abstract principles towards operational expectations for AI. By framing GDPR and AI Act obligations as structurally linked and lifecycle-wide, the guidance offers a practical supervisory lens on how privacy and AI governance are expected to converge in practice.

Global landscape of privacy and Artificial Intelligence

Artificial Intelligence and privacy: A global governance overview

Europe

Binding AI Act + GDPR foundation.

Risk-based, rights-focused global benchmark.

United States

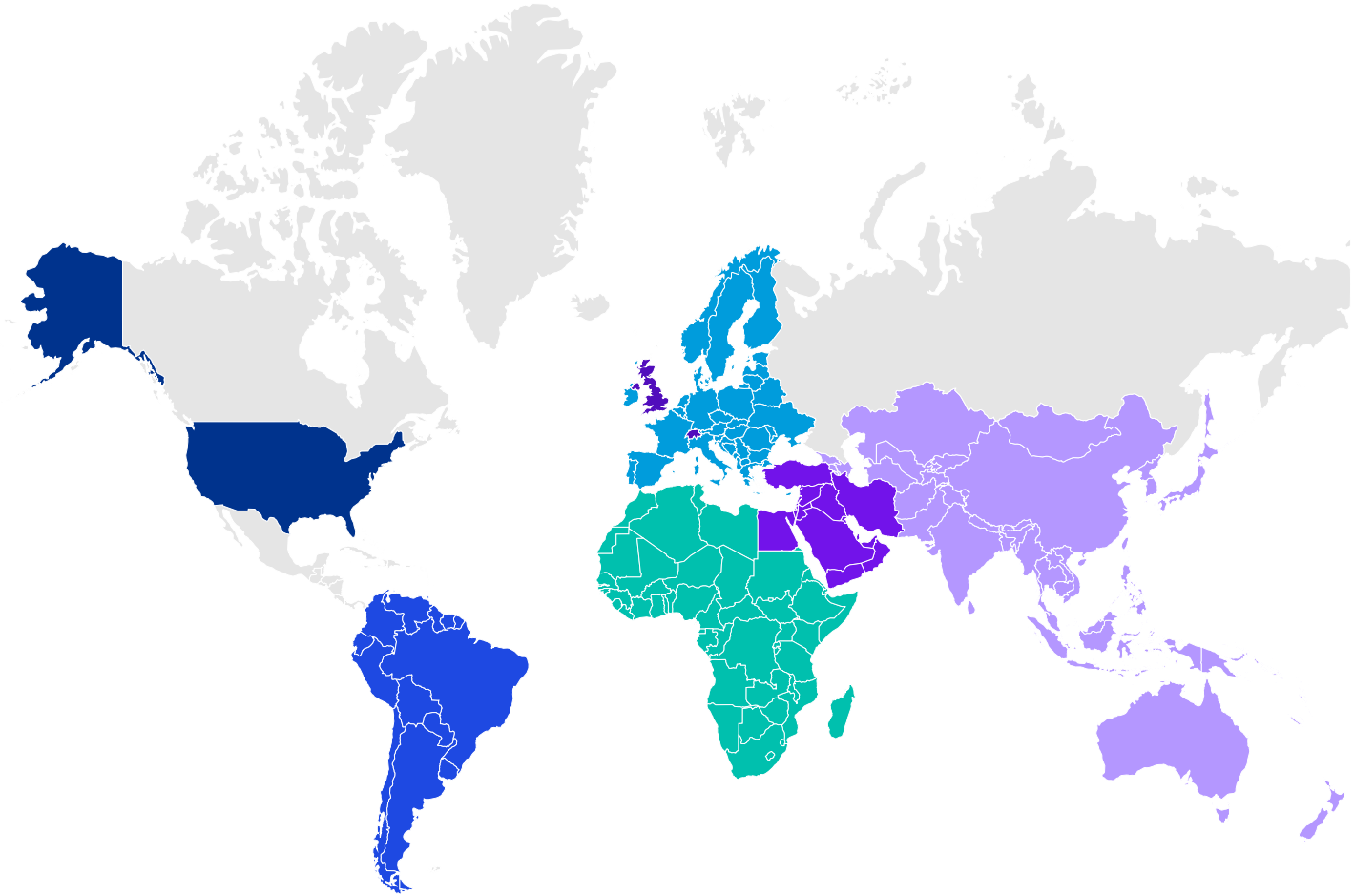
No federal AI law.

State privacy acts + sectoral enforcement (FTC, FDA, SEC, DoT).

Latin America

Mixed progress.

Brazil leads with LGPD and a new AI bill, while Peru has adopted a national AI legal framework focused on ethical and responsible use. Other countries continue pursuing privacy and AI related reforms.



UK / Switzerland

Advancing their own AI frameworks; closely aligned with European standards.

Middle East

AI central to national strategies.

UAE centralised model; privacy varies.

Asia-Pacific

Highly varied.

China strict; Japan voluntary; SK, India emerging; Singapore advanced model framework.

Africa

Developing principles.

Nigeria and South Africa advancing AI governance.

Global landscape of privacy and Artificial Intelligence

Artificial Intelligence and privacy: A global governance overview

Three key privacy challenges and potential benefits:

Common principles

Transparency / Accountability / Security

Regional approaches diverge

EU leads with binding frameworks (GDPR, AI Act); US relies on state laws and agencies (FTC); Asia-Pacific mixes strict rules with voluntary models; Latin America and Africa show early progress.

Regulatory fragmentation

raises compliance costs and limits global interoperability. **Privacy professionals** play a critical role in helping to mitigate these effects by fostering alignment across jurisdictions and assisting with embedding consistent privacy and AI governance practices within their organizations.

> "In an era where Artificial Intelligence is helping to reshape economies and societies, governance frameworks should keep pace, not only to help drive innovation but also to safeguard privacy and fundamental human rights."

Global landscape of privacy and Artificial Intelligence

Global trends

Despite regional differences, KPMG Spain conducted an analysis in September 2025 that identified several common trends at the intersection of artificial intelligence and privacy:

01 Privacy as a Cross-Cutting Principle

Privacy should not be considered a standalone domain; indeed, it is now a **foundational requirement** embedded throughout the AI lifecycle: from model design and dataset selection to result validation and production monitoring.

02 From Generative to Agentic AI

The rise of generative models has prompted swift responses from regulators and data protection authorities. These actions reinforce the AI Act's provisions on transparency, traceability, and legality in training datasets, showing how concerns over the use of personal data and algorithmic bias are intensifying.

Building on this, attention is now shifting toward **agentic AI systems**, autonomous, goal-directed models capable of acting on behalf of users or organizations. This evolution raises new privacy and accountability challenges, particularly around continuous learning, contextual decision-making, and the need for stronger governance and human oversight frameworks.

Alongside this technological shift, emerging paradigms such as hybrid and self-adaptive AI continue to drive further debates about autonomy, feedback loops and control.

03 Risk of Regulatory Fragmentation

While core principles are converging, regulatory implementation progresses at uneven speeds. Reports from different institutions warn of a "regulatory balkanization" that increases compliance costs and hinders global interoperability. This trend is also shaped by sovereignty considerations, with jurisdictions competing to become global leaders in AI.

04 Strengthening Transparency and Accountability

Authorities are demanding algorithmic explainability, human oversight mechanisms, and auditability of operational AI systems. Transparency is evolving from an ethical ideal to an operational imperative.

05 Emerging International Cooperation

Organizations are advancing global reference frameworks. The **Council of Europe AI Treaty (2024)** represents the first binding international treaty on AI, reinforcing the global momentum toward common standards. While no single binding international framework exists yet, these initiatives lay the groundwork for greater global interoperability.

Global principles for Trusted AI: Integrating ethics, privacy and accountability

Global principles for Trusted AI: Integrating ethics, privacy and accountability

Trusted AI: A human-centric and trustworthy approach to AI development that addresses ethical concerns and complies with regulatory standards

Given the international landscape where privacy is recognized as a fundamental and integral component of artificial intelligence, it is essential to adopt frameworks that integrate **best practices** and provide **global guidance**.

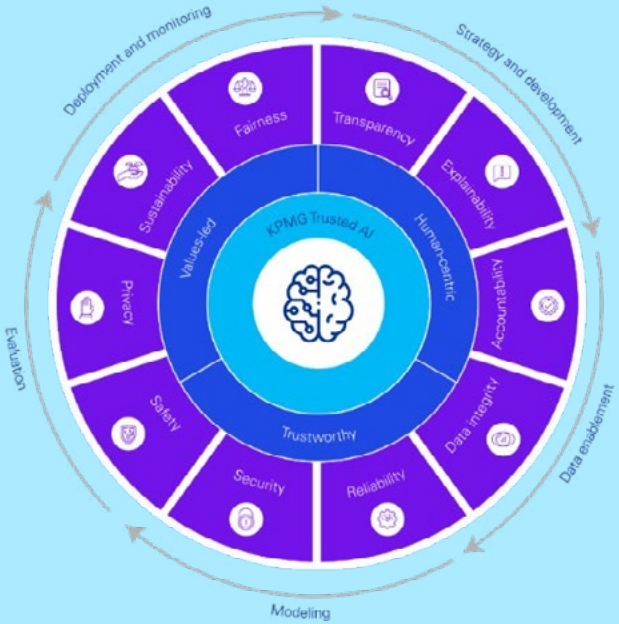
In this context, and drawing on member firms' professionals experience, KPMG has developed **Trusted AI framework** that outlines key principles which seek to ensure AI implementation is responsible, secure, and aligned with the strategic objectives of the organization.

Global principles for Trusted AI: Integrating ethics, privacy and accountability

Trusted AI: A human-centric and trustworthy approach to AI development that addresses ethical concerns and complies with regulatory standards

This framework is a **practical approach** that helps organizations navigate and integrate the multitude of existing international and local requirements in a harmonized and scalable way. It addresses ethical and operational risks at every stage of the AI lifecycle, supporting mitigation and control.

AI solutions should be designed to comply with applicable privacy and data protection laws and regulations.



The KPMG Trusted AI framework is aligned with leading regulatory and standards frameworks in the field of artificial intelligence and risk management, including ISO/IEC 42001; NIST AI Risk Management Framework; European Union's AI Act; OECD AI Principles; General Data Protection Regulation (GDPR).

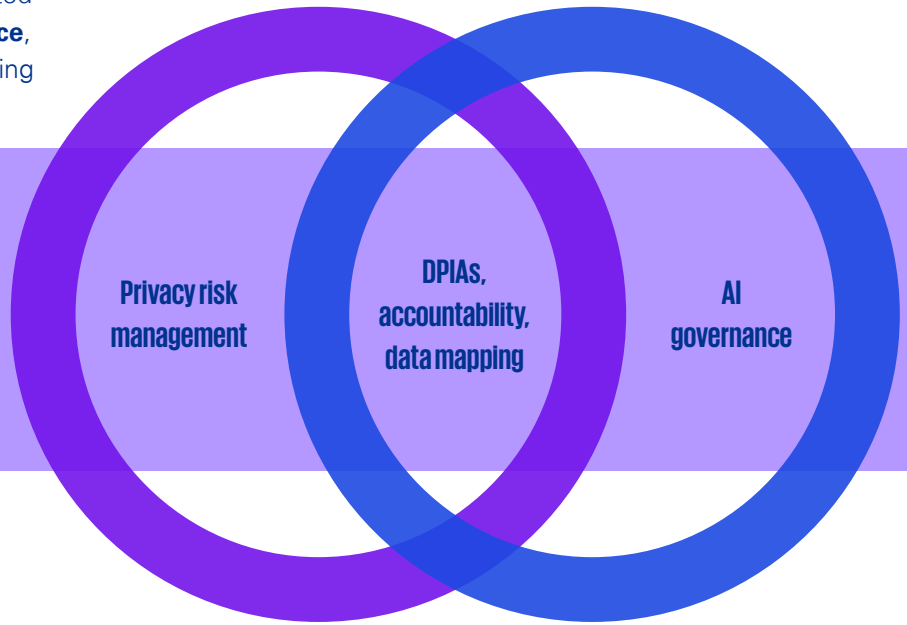
Global principles for Trusted AI: Integrating ethics, privacy and accountability

Trusted AI: A human-centric and trustworthy approach to AI development that addresses ethical concerns and complies with regulatory standards

AI solutions should be designed to comply with applicable privacy and data protection laws and regulations.

To support this the KPMG Trusted AI framework, provides a structured approach to AI governance through a series of principles and controls aimed at ensuring systems are developed and operated in a responsible, ethical, and transparent manner. To address the **risk of privacy non-compliance**, frameworks require **Data Protection Impact Assessments (DPIAs)** prior to deployment, ensuring that inherent and residual risks are properly assessed.

The connection between privacy risk management and AI governance demonstrates that GDPR compliance activities—like conducting data protection impact assessments, data mapping, and establishing accountability measures—can provide a basis for fulfilling AI Act requirements and supporting trustworthy AI.



DPIAs serve as an analytical tool, with resulting mitigation measures addressed through complementary processes. In addition, **trustworthy AI** demands continuous reviews and monitoring across the lifecycle to identify emerging risks and maintain accountability.

Within organizations, **DPOs should be playing a pivotal role in operationalizing these principles**, ensuring that privacy, accountability and transparency requirements are effectively embedded into AI governance structures.

As it will be explored further in this paper, **one of the key pillars of this approach is the integration of privacy from the design phase and throughout the entire lifecycle of the AI system**, with the aim of ensuring that emerging privacy risks are systematically identified and addressed withing a trusted governance model.

Global principles for Trusted AI: Integrating ethics, privacy and accountability

Trusted AI: A human-centric and trustworthy approach to AI development that addresses ethical concerns and complies with regulatory standards

Trusted AI identifies **two primary privacy risks associated with the use of AI systems**

Building on **Trusted AI Framework**, it is essential to understand the key privacy risks that can undermine the ethical and responsible use of AI. Identifying and addressing these risks is critical to maintain trust and ensuring compliance with emerging regulatory frameworks.

Privacy Compliance Risk

Failure to comply with regulatory requirements and best practices for privacy (e.g. inappropriate collection/ disclosure of personal data) may result in a loss of consumer trust, regulatory non-compliance, or cause financial harm.

Privacy Violations from AI Solutions

Failure to comply with Organization Privacy Directives and Procedures and applicable laws and regulations (e.g. Illegitimate use of personal data in AI training models) may result in a loss of consumer trust, regulatory non-compliance, or cause financial harm.

This approach can not only mitigate privacy risks but can also strengthens user trust in AI solutions, enhancing adoption and promoting safe use of the technology.

This is further evidenced by the **EU AI Act**, which identifies **eight categories of "high-risk" AI systems**, seven of which inherently **involve the processing of personal data**. This illustrates that most AI-related risks, from bias and discrimination to lack of transparency or accountability, ultimately originate from how personal data is collected, used, or governed.

As AI Systems evolve toward **more autonomous** and **agentic forms**, new privacy challenges emerge. These include the use of **sensitive data** without appropriate safeguards, **automated decision-making** without sufficient human oversight, and **reliance on third-party data sources** that can introduce bias or inaccuracies. Such systems require robust governance and continuous monitoring to maintain accountability and transparency.

To mitigate these risks, international standards such as ISO/IEC 42001 **AI-specific risks, such as bias**; particularly when personal data **fails to reflect population diversity** or is **used in a discriminatory manner**. Aligning with this approach, **Trusted AI Framework** supports organizations in embedding privacy, ethical principles, and accountability mechanisms throughout every stage of the AI lifecycle, helping ensure that AI systems remain secure, explainable and trustworthy.

This alignment between privacy, ethics, and accountability at the organizational level mirrors the broader global movement toward human-centric and rights-based AI governance.

Global principles for Trusted AI: Integrating ethics, privacy and accountability

Embedding privacy in global AI governance

Placing **individuals at the center of AI development** requires that all technology solutions and regulations **uphold human rights**, where privacy should remain a central pillar across the entire AI lifecycle.

The UN Global Digital Compact[7] highlight **AI's potential to deliver major societal benefits** (such as advancing science, democratizing knowledge, and improving decision-making) while stressing the **need for clear boundaries, ethical safeguards, and respect for privacy as a fundamental right**.

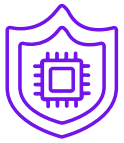
Ensuring that the use of personal data aligns with international legal principles. In particular, the European Convention on Human Rights (article 8) establishes that the development, training, testing, governance, and use of AI systems that process persona datal should fully respect individuals' right to private and family life.

> "International organizations have made this message clear: human rights should be integrated throughout the AI lifecycle including privacy."

Global principles for Trusted AI: Integrating ethics, privacy and accountability

Embedding privacy in global AI governance

UNESCO, alongside governments and private sector stakeholders, reached consensus on the following priorities:



Integrating privacy safeguards across the AI lifecycle

Conducting continuous security and risk assessments

Promoting multilateral cooperation and inclusive participation

Raising public awareness to foster education and accountability

Given these priorities, it is recommended to **establish policies that ensure privacy is protected as AI technologies continue to advance rapidly**.

The report recommends **the use of frameworks and tools** to detect biases, mitigate risks, and address the potential for large-scale surveillance enabled by AI-driven data collection. In line with the Universal Declaration of Human Rights, organizations should apply **proactive organizational accountability** across AI systems, going beyond Privacy by Design/Default to encompass broader governance measures such as oversight, delegation of authority, and compliance mechanisms.

As AI systems become more embedded in decision-making and everyday operations, privacy should be operationalized across all stages, from design and training to deployment and oversight, to ensure that privacy is not an abstract commitment, but a practical safeguard guiding real implementation.

In summary, privacy and data protection are foundational to the ethical and responsible development of AI technologies. It is imperative to embed privacy from the design phase and throughout the entire lifecycle of AI systems.

Global principles for Trusted AI: Integrating ethics, privacy and accountability

From principles to practice operationalizing PbD in AI

Building on this global consensus around human rights and ethical safeguards, the next step is to understand how these principles translate into practice. As organizations move from commitment to implementation, privacy should become a practical design and governance requirement throughout the AI lifecycle.

Frameworks such as **ISO/IEC 27701** and the **NIST AI Risk Management Framework** (AI RMF) provide concrete methods to embed privacy and accountability in AI system, transforming abstract principles into measurable actions. These frameworks enable organizations to minimize data collection, configure privacy by default, strengthen security, and ensure transparency across every stage of AI development and operation.

The concept of Privacy by Design (PbD) underpins this approach. Originating in the 1990s, established the idea that privacy should be proactively embedded into technologies and processes. Its principles: proactivity, data minimization, security, and transparency, have shaped today's global standards, influencing frameworks such as the **OECD AI Principles** and the **EU GDPR**.

For privacy professionals and DPOs, this evolution expands their role: from ensuring regulatory compliance to actively contributing to AI risk governance, data mapping, and impact assessments. By bridging privacy and AI compliance, they can help operationalize trustworthy AI.

This alignment is clearly reflected in the Privacy in the new world of AI KPMG International. How to build trust in AI through privacy[22], which outlines how privacy can serve as a strategic enabler of trust in AI systems.

Global principles for Trusted AI: Integrating ethics, privacy and accountability

From principles to practice operationalizing PbD in AI

	OECD AI principles				
	• Accountability	• Inclusive growth, sustainable development and wellbeing	• Human-centered values and fairness	• Transparency and explainability	• Robustness, security and safety
GDPR principles	• Accountability	• Purpose limitation • Data minimization	• Lawfulness, fairness and transparency • Purpose limitation • Accuracy • Storage limitation	• Lawfulness, fairness and transparency	• Integrity and confidentiality
Privacy by Design principles	• Proactive not reactive; preventative not remedial	• Privacy embedded into design • Full functionality – positive-sum, not zero-sum	• Privacy as the default setting • Respect for user privacy – keep it user-centric	• Visibility and transparency – keep it open	• End-to-end security – full lifecycle protection

Privacy in the New World of AI: How to Build Trust in AI Through Privacy, KPMG International, 2024.

The OECD AI Principles and the Privacy by Design (PbD) approach are grounded in the same foundational idea: **privacy and fundamental rights** should be **embedded into technology from the outset**.

Although the term gained prominence with the introduction of the GDPR, the **principle is reflected across various international frameworks and legal instruments that impose obligations to integrate privacy throughout the AI lifecycle**. For instance, while the CCPA/CPRA does not explicitly reference PbD, it establishes data minimization as a core principle requiring systems to be configured to limit unnecessary exposure to personal data from the beginning.

Another example is found in Canada, where both **PIPEDA** and the **Privacy Act** promote the "fair information principles," encouraging the integration of privacy controls from the design phase.

Privacy across the AI lifecycle

Privacy across the AI lifecycle

Privacy as a continuous process in AI governance

As previously outlined, **privacy should not be confined to just the technical development phase of AI systems**. Instead, it should be integrated into every stage of the system's lifecycle, including initial planning and design, operation, oversight, and final decommissioning. That's why **privacy professionals should be involved** throughout the entire process. **Only by treating privacy as a continuous process can AI systems be built** that are **trustworthy**, **legitimate**, and **sustainable**.

As can be seen throughout the first sections of this document, both the **current regulation** and the **future regulatory framework for AI** are expected to be **supported by countries and territories data protection legislation**, on the following pages we outline the **key takeaways** that should be considered at each stage.

Privacy across the AI lifecycle

Privacy as a continuous process in AI governance

01

Design and test phase: Embedding privacy from the start

The foundation of trustworthy AI begins at the design stage. Ensuring privacy and data protection from the outset is not just a compliance exercise, it is a strategic requirement to build systems that are ethical, robust, and aligned with business objectives. Working to reduce risks at this phase can help to avoid costly corrections later and strengthens public trust.

Before production, **insufficient testing** or **underdeveloped AI systems** may result in errors, which can cause inaccurate outcomes, incorrect decisions, and lower reliability, ultimately increasing risks to proper operation.

Key priorities at this stage include:

Data minimization Limit the collection and use of personal data. Use only the data necessary for testing, avoiding excessive collection and ensuring that the information is relevant to the test objectives.

Quality and accountability Document training processes, sources, and methodologies to ensure compliance and enable audits.

Anonymization and pseudonymization If it is necessary to use personal or specially protected data, adopt appropriate safeguards to protect it and reduce the risk of exposing personal information.

Bias prevention Avoid non-representative or poor-quality datasets that could lead to discriminatory outcomes.

Synthetic and anonymized data Prioritize secure alternatives that reduce privacy risks, like re-identification.

Performance evaluation Integrate continuous monitoring to ensure effectiveness and robustness of AI systems.

Privacy across the AI lifecycle

Privacy as a continuous process in AI governance

02

Production phase: Security, transparency and user rights

Once deployed, **AI systems should guarantee** not only **functionality but also security, accountability, and respect for individuals rights**. The production phase is critical to ensure traceability, resilience against threats, and user trust.

Essential safeguards at this stage could include:

Robust security controls Protect against data manipulation, tampering, hallucinations, re-identification, and fraud, among others.

Traceability and logging Ensure system activity can be audited and monitored effectively.

User rights Guarantee access, correction, and control over personal data throughout the lifecycle.

03

Retraining and Continuous Improvement: Reassess Legal Bases and Consent

Continuous improvement requires adapting AI systems to evolving internal and external contexts. This stage is not only refining models but also about reinforcing transparency and ensuring renewed user consent is aligned with privacy regulations.

Critical enablers for this stage include:

Clear communication to users about how their data is used and the consequences of AI systems.

Mechanisms to obtain renewed consent whenever retraining occurs.

Periodic adjustments of AI systems to reflect new risks or regulatory requirements.

Risk assessment continuously identify vulnerabilities and assess impact to anticipate threats.

Privacy across the AI lifecycle

Privacy as a continuous process in AI governance

04

Governance: The Role of Human Oversight

Trustworthy AI should remain under human control, even in highly automated environments. Governance at this stage ensures accountability, security, and protection of individuals rights through robust oversight mechanisms.

Fundamental safeguards are:

Guaranteeing AI systems remain subject to **meaningful human control** and **human supervision** (human-in-the-loop)

Continuous lifecycle monitoring and audits in accordance with **ISO/IEC 27701** and **ISO/IEC 42001** enable us to **build on security as a foundation**, while **extending** the framework to include **trust**, **accountability**, and **ethics in AI systems**.

Upholding individuals' rights to **consent automated decisions** and **request human intervention**.

Ensure responsible decommissioning. If needed, shutting down the AI system on a responsible way, ensuring that all data and risks are managed appropriately and that traceability is maintained during the process.

This approach enables a proactive risk management strategy addressing risks throughout the entire AI lifecycle, from design conception to deployment and ongoing operation.

Conclusions

Conclusions

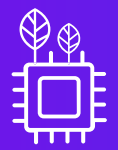
Privacy and trust: The foundation of ethical AI

Privacy is the cornerstone of trustworthy, ethical and legitimate AI.

Embedding privacy across the lifecycle promotes transparency, accountability, and non-discrimination.

Regulation does not hinder innovation; it accelerates it and strengthens public trust.

The Trusted AI approach ensures privacy is present from design through continuous oversight



Balancing technological progress with fundamental rights is the foundation of sustainable AI.

Multiple developer experiences help to demonstrate that privacy is far more than a legal requirement; it has become a structural principle that should be embedded throughout the entire lifecycle of AI systems.

Despite these conclusions, many organizations can still face key challenges. To help address them, the following recommendations should be considered essential:

From design to deployment: Strengthen Privacy by Design – such as data minimization, bias testing and synthetic datasets, among others.

Continuous oversight: Implement audits and monitoring (ISO/IEC 42001, GDPR art. 22) to help ensure compliance and accountability.

Generative AI risks: Define safeguards for training data, re-identification, and algorithmic transparency.

Human in the loop: Guarantee the right to meaningful human oversight in automated decisions.

Global cooperation: Reduce regulatory fragmentation by aligning with emerging global standards (OECD, UNESCO, UN).

Internal support: Privacy professionals should seek allies within their organizations to strengthen security measures in AI environments, as well as the quality and use of personal data.

Contacts

Benny Bogaerts
Partner Digital Risk Management
KPMG in Belgium
bbogaerts@kpmg.com

Johanna Vandervorst
Senior Advisor,
Digital Risk Management
KPMG in Belgium
jvandervorst@kpmg.com

Contributors

Oskar Trpisovsky
GTA Privacy LeaderRisk Services – Cyber Security
KPMG in LLP
otrpisovsky@kpmg.ca

Orson B. Lucas
Principal, Advisory Offering,
Risk Services
KPMG in US
olucas@kpmg.com

Ethan Yin
Associate Director
BJW TECHTR Cyber ITRA
KPMG in China
ethan.yin@kpmg.com

Stephan Idema
Director
Tech Law & Privacy
KPMG in Netherlands
Idema.Stephan@kpmg.nl

Javier Aznar
Partner,
Technology Risk
Cybersecurity and Privacy
KPMG in Spain
jaznar@kpmg.es

Ángela Manceñido
Senior Manager
Technology Risk
Cybersecurity and Privacy
KPMG in Spain
amancenido@kpmg.es

María Cristina Köhler
Manager
Technology Risk
Cybersecurity and Privacy
KPMG in Spain
mariacristinakohler@kpmg.es

2026
KPMG International | kpmg.com

References to documentation and paperwork

[1] G7, Council of Europe, United Nations: Global Governance and Corporate Responsibility, Council on Foreign Relations, Council of Europe, United Nations, 2024.

[2] OECD AI Principles, OECD, updated version 2024.

[3] Executive Orders and Presidential Actions, The White House, Office of the President of the United States, updated version, 2025.

[4] Aiming for Truth, Fairness, and Equity in Your Company's Use of AI, Federal Trade Commission (FTC), 2021.

[5] Recommendation on the Ethics of Artificial Intelligence, UNESCO, 2021.

[6] Office of the United Nations High Commissioner for Human Rights (OHCHR): Mandate and Leadership, United Nations Human Rights Office

[7] Global Digital Compact: Governance of Emerging Technologies, United Nations, Office for Digital and Emerging Technologies, 2024.

[8] Understanding the intersection between the EU's AI Act and privacy compliance, Compact Magazine, KPMG Netherlands, 2024

[9] U.S. Securities and Exchange Commission (SEC): Investor Protection and Market Integrity, Securities and Exchange Commission

[10] Centre for Connected and Autonomous Vehicles (CCAV): Innovation in Mobility and Transport Policy, UK Government, Department for Transport & Department for Business and Trade

[11] UAE Strategy for Artificial Intelligence 2031: Transforming Government Services through Emerging Technologies, United Arab Emirates Government, Ministry of Artificial Intelligence, updated version, 2025.

[12]ICO Consultation Series on Generative AI and Data Protection, Information Commissioner's Office (ICO), United Kingdom, September 2024.

[13] Annual Report 2023–2024, World Economic Forum, 2024.

[14] Market Concentration Implications of Foundation Models: The Invisible Hand of ChatGPT, Brookings Institution, Center on Regulation and Markets, 2023.

[15] Governing AI for Humanity: Final Report, Advisory Body on Artificial Intelligence, United Nations, 2024.

[16] International Chamber of Commerce: Global Business Leadership and Policy Engagement, International Chamber of Commerce (ICC), 2025.

[17] Annual Report 2020, UK Information Commissioner's Office (ICO), 2020.

[18] Deploying truswothy AI: An Illustrative Risk and Controls Guide, KPMG International, 2025

[19] 53rd Regular Session of the Human Rights Council, United Nations, Office of the High Commissioner for Human Rights, 2023.

[20] 2nd Global Forum on the Ethics of Artificial Intelligence: Shaping AI Governance, UNESCO and Government of Slovenia, 2024.

[21] Assessing Potential Future Artificial Intelligence Risks, Benefits and Policy Imperatives, OECD, 2024.

[22] Privacy in the New World of AI: How to Build Trust in AI Through Privacy, KPMG International, 2024.

Regulatory references

EU AI Act - European Union

General Data Protection Regulation (GDPR) - European Union

California Consumer Privacy Act (CCPA) - California

NIST SP 800-53 Control Overlays for Securing AI Systems

Blueprint for an AI Bill of Rights - EEUU

General Personal Data Protection Law (LGPD) - Brazil

Proyecto de Ley N° 2338/23 - Brazil

AI Risk Management Framework, National Institute of Standards and Technology (NIST), versión 1.0, 2023

Universal Declaration of Human Rights

European Convention on Human Rights

Guia de la Agencia Española de Protección de Datos - Spain

Guidelines on AI Security - Singapore

Artificial Intelligence and Data Act - Canada

ISO 42001 Gestión Inteligencia Artificial

Projeto de Lei nº 233/2023: Inteligência Artificial e Direitos Fundamentais, Senado Federal do Brasil, Comissão de Ciência e Tecnologia, 2025 - Brazil

Model AI Governance Framework (Second Edition), Personal Data Protection Commission (PDPC), Singapore Government, 2020

Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, Council of Europe, adopted version, 2024

Labeling Rules for AI-Generated Content, Cyberspace Administration of China, adopted version, 2025

Interim Measures for the Management of Generative Artificial Intelligence Services - Cyberspace Administration of China. (2023, July 13).

ISO/IEC 42001:2023 – Artificial Intelligence Management System, International Organization for Standardization / International Electrotechnical Commission, 2023

ISO/IEC 27557:2024 – Privacy in AI Systems, International Organization for Standardization / International Electrotechnical Commission, 2024

The Personal Information Protection and Electronic Documents Act (PIPEDA) - California

Privacy Act - Canada

Global AI Governance Action Plan - China

Act on the Protection of Personal Information Act No. 57 of 2003) (APPI) - Japan

National Status Report on AI Safety in Japan - Japan

Personal Information Protection Law of the People's Republic of China - China

Cybersecurity Law of the People's Republic of China - China

Data Security Law of the People's Republic of China - China

The Digital Personal Data Protection Act, 2023 (No. 22 Of 2023) (DPDPA) - India

Report on AI Governance Guidelines Development - India

Protection of Personal Information Act (POPIA) - South Africa

AI Blueprint - Africa

NIST Privacy Framework and AI Risk Management Framework, National Institute of Standards and Technology, 2023