AI & Partners

Amsterdam - London - Singapore

EU AI Act

OECD AI Principles versus EU AI Act

A Mapping Exercise

April 2025

AI & Partners

Sean Musch, AI & Partners

Michael Borrelli, AI & Partners

Charles Kerrigan, CMS UK

Sigrid Berge van Rooijen, Eir Health

Lord Holmes of Richmond, UK House of Lords

Principles

EU AI Act

VS

OECD

BETTER POLICIES FOR BETTER LIVES

AI & Partners

Amsterdam - London - Singapore

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/.

Contact: Michael Charles Borrelli | Director | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

OECD
BETTER POLICIES FOR BETTER LIVES

Contents

Introduction

As artificial intelligence continues to transform industries, businesses must adopt structured governance frameworks to ensure ethical, transparent, and responsible AI deployment. The EU AI Act and OECD AI Principles provide critical guidance for organizations seeking to align AI systems with fundamental rights, safety standards, and democratic values. These frameworks emphasize risk management, human oversight, and accountability, ensuring AI operates in a trustworthy and legally compliant manner.

This report explores the core principles, regulatory implications, and best practices for implementing AI governance under the EU AI Act and OECD AI Principles. From risk assessments to transparency measures, these frameworks offer businesses a roadmap for fostering responsible AI innovation while mitigating potential harms.

With increasing regulatory scrutiny and global AI policies evolving rapidly, organizations must demonstrate AI governance maturity to maintain compliance and public trust. Adopting the EU AI Act's risk-based approach, alongside the OECD's values-driven principles, helps businesses ensure AI aligns with ethical and legal expectations, reducing liability risks and enhancing system reliability.

Whether you are an AI developer, business leader, or policymaker, this report serves as a strategic resource for implementing responsible AI governance. At AI & Partners, we remain committed to supporting organizations in building AI that is ethical, accountable, and aligned with international standards.

Best regards,

Sean Musch

Founder/CEO

AI & Partners

Key questions being asked about OECD AI Principles

1. What are the OECD AI Principles, and why are they important?

The OECD AI Principles provide an internationally recognized framework for the ethical and responsible development of AI. They emphasize inclusive growth, human rights, transparency, robustness, and accountability, ensuring AI benefits society while mitigating risks. Adopted by over 40 countries, these principles guide policymakers and businesses in aligning AI development with democratic values and ethical standards. Promoting trustworthy AI means the principles help balance innovation with human-centric values, encouraging AI applications that support fairness, sustainability, and economic prosperity while minimizing harm. They serve as a foundation for AI regulations worldwide, including the EU AI Act.

2. How do the OECD AI Principles influence the EU AI Act?

The EU AI Act integrates many key aspects of the OECD AI Principles, reinforcing transparency, accountability, and human-centric AI development. Both frameworks emphasize AI safety, human oversight, and risk-based governance, ensuring AI systems operate within ethical and legal boundaries. The EU AI Act expands on these principles by legally enforcing compliance, requiring impact assessments, documentation, and risk mitigation for high-risk AI applications. Aligning with OECD guidelines permits the Act to ensure global interoperability in AI governance, enabling businesses to navigate AI regulations while fostering ethical and sustainable AI innovation.

3. How do the OECD AI Principles promote transparency in AI systems?

Transparency is a core tenet of the OECD AI Principles, ensuring that AI users and stakeholders understand how AI systems make decisions. The principles advocate for explainability, requiring AI developers to provide clear, accessible information about data usage, system logic, and decision-making processes. Transparency also includes disclosure obligations, such as informing users when they interact with AI-powered systems. These measures enhance public trust and ensure that AI decisions can be challenged when necessary, preventing black-box AI models from operating without accountability.

4. How do the OECD AI Principles ensure AI contributes to inclusive growth?

The OECD AI Principles highlight AI's potential to drive inclusive growth, sustainable development, and well-being. They encourage AI innovation that benefits all of society, rather than deepening inequalities. This includes ensuring AI expands opportunities for underrepresented communities, promotes economic fairness, and reduces biases in decision-making. Embedding inclusivity into AI policies and business strategies allows organizations to create AI that empowers diverse populations, improves access to essential services, and supports environmental sustainability—helping bridge the digital divide rather than exacerbate existing disparities.

5. Why is accountability crucial in AI governance according to the OECD AI Principles?

Accountability ensures that AI developers, operators, and users take responsibility for AI outcomes. The OECD AI Principles call for clear governance structures, requiring organizations to document AI decisions, assess risks, and establish human oversight. This means that when AI systems cause harm—whether through bias, security failures, or ethical violations—those responsible must provide explanations and corrective actions. Accountability also involves collaborative governance, where businesses, regulators, and civil society work together to ensure AI remains aligned with human values and legal standards.

6. How do the OECD AI Principles address AI security and robustness?

AI systems must be resilient, secure, and safe to function reliably in diverse conditions. The OECD AI Principles emphasize the need for robust AI design, ensuring systems can withstand adverse scenarios, cybersecurity threats, and unintended failures. This includes continuous risk monitoring, impact assessments, and security audits to prevent AI misuse. Organizations are encouraged to implement fail-safes and human intervention mechanisms, ensuring AI does not operate autonomously in ways that could endanger users. These safeguards protect against AI vulnerabilities while fostering trust in AI adoption.

7. How do the OECD AI Principles safeguard human rights in AI development?

The OECD AI Principles stress that AI should respect fundamental human rights by ensuring fairness, privacy, and non-discrimination. AI must not reinforce social biases, engage in mass surveillance, or infringe on freedoms such as autonomy and dignity. Developers are expected to integrate ethical guidelines, diverse datasets, and human-centric oversight to prevent AI from harming marginalized groups. AI actors should also implement redress mechanisms so that individuals can challenge harmful AI-driven decisions, ensuring legal protections remain intact in an AI-powered world.

8. How do the OECD AI Principles encourage human oversight of AI systems?

AI should augment, not replace, human decision-making in critical areas like healthcare, law enforcement, and financial services. The OECD AI Principles advocate for "human-in-the-loop" systems, where trained professionals oversee AI decisions, intervene when necessary, and prevent automated harm. Human oversight is particularly important in high-stakes applications, ensuring AI does not make life-altering choices without appropriate checks. Businesses implementing AI should establish clear governance protocols, defining when, how, and to what extent humans should supervise AI operations to maintain ethical and accountable AI use.

9. How can businesses align their AI strategies with the OECD AI Principles?

Businesses should embed OECD AI Principles into their AI governance frameworks by ensuring transparency, risk management, and fairness at every stage of AI development. This includes:

- Conducting ethical AI impact assessments to prevent biases and ensure inclusivity.
- Providing clear explanations of AI decisions to users and regulators.
- Developing risk management systems that monitor AI safety and security.
- Collaborating with regulators and industry bodies to align with evolving AI policies. By integrating these principles, businesses can enhance trust, legal compliance, and sustainable AI innovation while avoiding reputational and regulatory risks.

10. How do the OECD AI Principles shape the future of AI governance?

As AI continues to evolve, the OECD AI Principles serve as a global reference for ethical AI regulation. Many governments and organizations—such as the EU, G7, and UN—are incorporating OECD guidelines into their AI policies, ensuring consistency across international regulations. Moving forward, AI governance will likely emphasize cross-border collaboration, stronger accountability frameworks, and AI safety mechanisms. Businesses adopting these principles early will be better positioned for regulatory compliance, ensuring they lead in trustworthy AI innovation rather than facing legal and ethical challenges down the line.

Understanding OECD AI Principles

Principle 1.1

Inclusive growth, sustainable development and well-being

What does it mean?

The OECD AI Principle 1.1 emphasizes that AI should promote inclusive growth, sustainable development, and overall well-being. This means ensuring AI benefits all individuals and societies rather than exacerbating inequalities. AI should support economic and social inclusion, protect the environment, and contribute to achieving global development goals, such as the UN Sustainable Development Goals (SDGs). Trustworthy AI should be designed to augment human capabilities, empower underrepresented populations, and reduce disparities, ultimately fostering a fairer and more sustainable future.

Why is it needed?

This principle is essential because AI has the potential to either bridge or widen global inequalities. Without intentional efforts, AI systems may reinforce existing biases and disproportionately impact vulnerable populations, including ethnic minorities, women, and low-income communities. Additionally, disparities in technology access could deepen divisions between developed and developing nations. As a result of ensuring AI contributes to inclusive growth and sustainability, we can harness its power to address societal challenges, support economic opportunity, and enhance environmental protection.

s

How can it be implemented?

Implementing this principle requires proactive policies, ethical AI design, and cross-sector collaboration. Governments should create regulations that promote AI-driven social and environmental benefits while mitigating risks. Organizations should integrate fairness, transparency, and inclusivity into AI development. Stakeholders, including policymakers, businesses, and civil society, should engage in public dialogue to ensure AI serves diverse communities. Additionally, investment in digital literacy, infrastructure, and equitable access to AI tools can help bridge gaps and create a more inclusive and sustainable AI ecosystem.

Principle 1.2

Respect for the rule of law, human rights and democratic values, including fairness and privacy

What does it mean?

The OECD AI Principle 1.2 emphasizes that AI systems must respect the rule of law, human rights, and democratic values. This means AI should be designed and deployed in a way that upholds fairness, privacy, non-discrimination, and individual autonomy. AI actors must ensure safeguards to prevent misuse, biases, and threats to freedoms such as privacy and freedom of expression. The principle calls for AI to align with human-centred values, ensuring it contributes positively to social justice, equality, and democratic governance.

Why is it needed?

This principle is necessary because AI has significant societal impacts, and without safeguards, it can infringe on fundamental rights. AI can perpetuate biases, invade privacy, or be misused for misinformation, surveillance, or discrimination. Ensuring AI aligns with democratic and human rights principles prevents harm, builds public trust, and fosters ethical AI development. With AI increasingly influencing governance, business, and daily life, maintaining fairness and legal protections helps create AI systems that enhance, rather than undermine, democratic and societal values.

How can it be implemented?

Implementation requires legal frameworks, ethical guidelines, and technical safeguards. Organizations should conduct fundamental rights impact assessments (FRIAs) and enforce human oversight mechanisms, such as keeping a “human in the loop” for critical AI decisions. Governments should set regulations ensuring AI fairness, transparency, and accountability. Industry standards, such as ethical codes of conduct and quality certifications, can further guide responsible AI development. Additionally, multidisciplinary collaboration and public dialogue can help shape AI policies that align with societal values and legal principles.

Principle 1.3

Transparency and explainability

What does it mean?

The OECD AI Principle 1.3 emphasizes transparency and explainability in AI systems. Transparency means that AI actors should disclose when AI is being used, whether in decision-making, recommendations, or user interactions. Explainability ensures that individuals affected by AI decisions can understand how those outcomes were reached. This principle promotes responsible disclosure, making AI systems more comprehensible while balancing feasibility, privacy, and security concerns. It enables stakeholders to trust AI by ensuring they have access to relevant information about its functioning.

Why is it needed?

Transparency and explainability are essential for trust, accountability, and fairness in AI. Without them, AI decisions may seem opaque or arbitrary, leading to public scepticism and potential harm. If users are unaware they are interacting with AI or cannot challenge AI-driven decisions, they may experience unfair outcomes. Transparency allows consumers, employees, and regulators to understand AI's role in society, while explainability ensures affected individuals can assess, question, and seek recourse against potentially biased or incorrect AI-generated outcomes.

How can it be implemented?

Implementing this principle requires clear communication strategies, technical solutions, and regulatory frameworks. AI developers should provide user-friendly explanations of AI decisions, including the main factors influencing outcomes. Organizations should disclose AI involvement in services, particularly in high-impact areas like hiring, finance, and healthcare. Regulators can establish guidelines requiring AI systems to provide explanations in proportion to their societal impact. Public awareness campaigns and multi-stakeholder dialogues can further ensure AI transparency, fostering trust while respecting privacy and intellectual property constraints.

Principle 1.4

Robustness, security, and safety

What does it mean?

The OECD AI Principle 1.4 emphasizes that AI systems must be robust, secure, and safe throughout their lifecycle. This means AI should function reliably under normal and adverse conditions, preventing harm from foreseeable misuse or unintended consequences. AI developers must integrate safeguards to detect and mitigate risks, ensuring AI can be overridden, repaired, or decommissioned if needed. Additionally, mechanisms should enhance information integrity while respecting freedom of expression, maintaining trust and security in AI-driven decision-making processes.

Why is it needed?

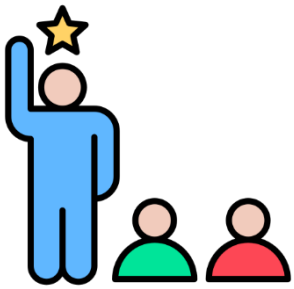
Ensuring robustness, security, and safety is essential because AI failures can result in significant harm, from cybersecurity threats to biased decision-making. AI systems interact with critical sectors like healthcare, finance, and infrastructure, where malfunctions can have serious consequences. Without safeguards, AI could be misused or exploited, leading to data breaches, misinformation, or even physical harm. Robust AI systems build public trust, reduce vulnerabilities, and ensure AI remains a beneficial tool rather than a source of uncontrolled risk.

How can it be implemented?

This principle can be implemented through a risk management approach, ensuring AI safety and security at every stage of development and deployment. Developers should conduct rigorous testing, monitor AI performance, and document risk mitigation strategies. Traceability measures, such as maintaining metadata records, can improve accountability and allow for analysis of AI outcomes. Governments should enforce safety regulations, while organizations should adopt cybersecurity best practices. Regular audits, human oversight, and ethical reviews can further ensure AI operates safely and responsibly.

Principle 1.5

Accountability



What does it mean?

The OECD AI Principle 1.5 emphasizes that individuals and organizations involved in AI development, deployment, and operation must be accountable for AI's proper functioning. This means AI actors should ensure transparency, risk management, and compliance with ethical and legal standards throughout the AI system lifecycle. Accountability includes maintaining traceability of data, processes, and decisions, allowing for oversight and corrections when necessary. It also involves collaboration among AI developers, suppliers, users, and other stakeholders to minimize risks and uphold responsible AI practices.

Why is it needed?

Accountability is crucial to ensure AI systems operate fairly, safely, and transparently. Without accountability, AI actors could evade responsibility for harmful biases, privacy violations, security risks, or other negative impacts. This principle promotes trust in AI by requiring developers and organizations to take responsibility for their systems' outcomes. In holding AI actors accountable, society can better address concerns like misinformation, discrimination, and ethical breaches, ensuring AI aligns with human rights, safety, and social justice values.

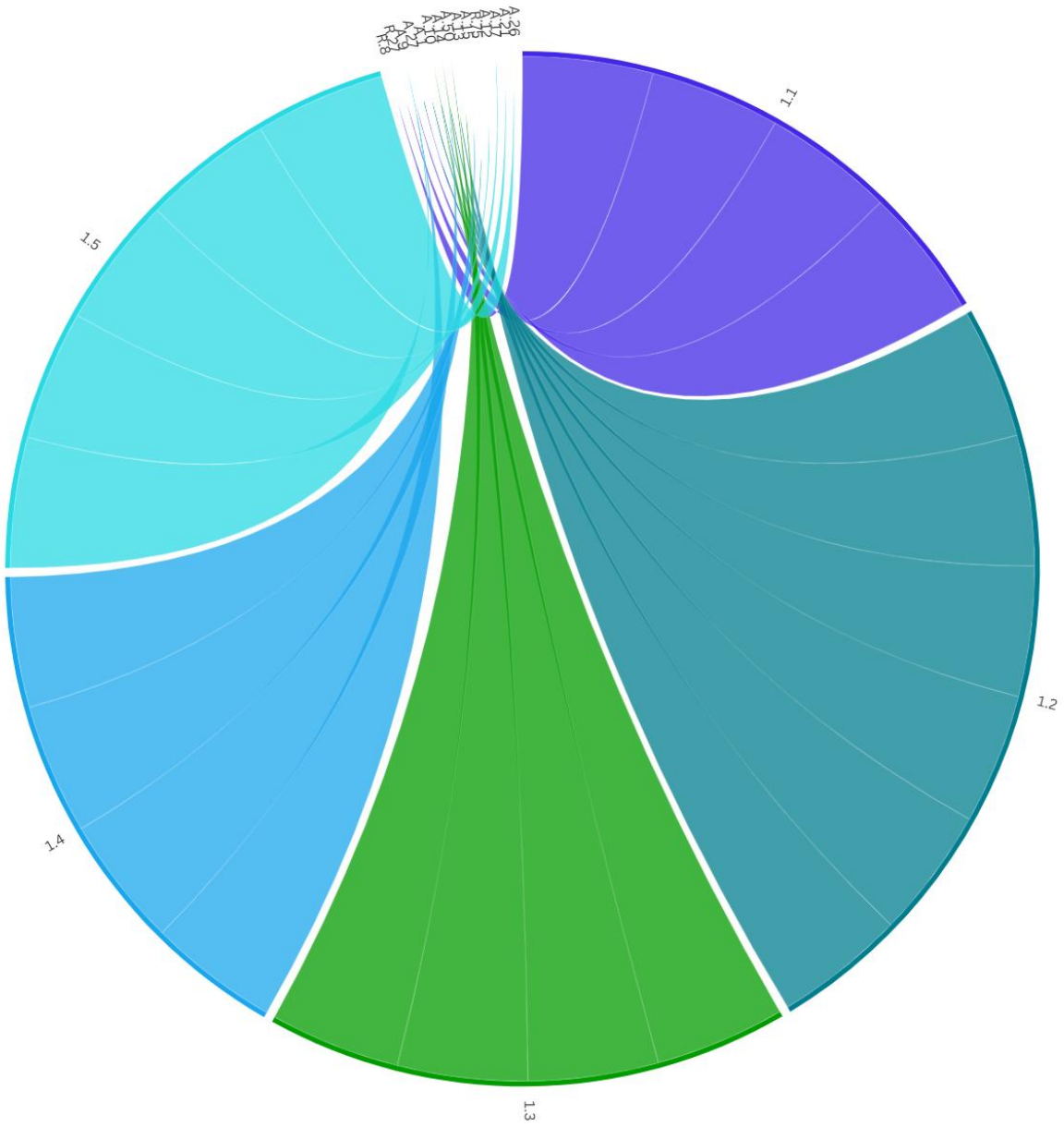
How can it be implemented?

Implementing accountability in AI requires clear regulatory frameworks, ethical guidelines, and internal governance policies. AI actors should document key decisions, conduct risk assessments, and enable audits to ensure compliance. Organizations should adopt responsible business practices, including transparency in AI development and ongoing monitoring for biases or security vulnerabilities. Governments can enforce accountability through laws and policies that define AI-related responsibilities and liabilities. Collaboration between AI developers, users, and regulators can further strengthen oversight, ensuring AI operates in a trustworthy and fair manner.

#

Mapping OECD AI Principles to EU AI Act

Striking a Chord: OECD AI Principles mapped against EU AI Act



Key:

- Larger end: OECD AI Principle
- Smaller end: EU AI Act provisions (Articles and Recitals)

OECD.AI		EU AI Act		
Principle	Description	Provision	Explanation	Action(s)
Inclusive growth, sustainable development and well-being (Principle 1.1)	This Principle highlights the potential for trustworthy AI to contribute to overall growth and prosperity for all – individuals, society, and planet – and advance global development objectives.	Recital 8	This recital emphasizes the need for a harmonized legal framework to foster AI development while ensuring high protection of public interests, such as health, safety, and fundamental rights. It highlights the importance of supporting innovative solutions and creating a European ecosystem for AI that aligns with Union values, including environmental protection.	**Engage in Ethical AI Development**: Businesses should integrate ethical guidelines into their AI development processes, ensuring that their systems promote inclusivity and sustainability. This involves considering the long-term social and environmental impacts of AI systems. **Participate in AI Regulatory Sandboxes**: Businesses, especially SMEs, should take advantage of AI regulatory sandboxes to test and refine their AI systems in a controlled environment. This participation can help ensure compliance with EU regulations and promote responsible AI innovation. **Implement a Risk Management System**: Develop a comprehensive risk management system that assesses and mitigates potential risks to fundamental rights, including social and environmental impacts. This aligns with the EU AI Act's emphasis on protecting public
		Recital 27	This recital underscores the importance of developing AI systems sustainably and in a manner that benefits all humans. It encourages stakeholders to consider ethical principles in AI development, which aligns with the OECD's focus on reducing inequalities and protecting the environment.	
		Article 9 (Risk management system)	Although not directly mentioned in the provided references, this article typically requires providers of high-risk AI systems to implement a risk management system that considers potential impacts on fundamental rights, which can include social and environmental considerations.	
		Article 57 (AI Regulatory sandbox)	This article supports innovation by providing a controlled	

			environment for developing and testing AI systems, with a focus on legal certainty and regulatory compliance. It aims to foster innovation while ensuring that AI systems are developed responsibly, which aligns with the OECD principle of responsible stewardship.	interests and fundamental rights.
Respect for the rule of law, human rights and democratic values, including fairness and privacy (Principle 1.2)	AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and should include appropriate safeguards to ensure a fair and just society.	**Article 1 (Subject matter)**	This article outlines the purpose of the EU AI Act, which includes promoting human-centric and trustworthy AI while ensuring a high level of protection for health, safety, and fundamental rights, such as democracy and the rule of law.	**Conduct Impact Assessments**: Businesses should perform fundamental rights impact assessments for their AI systems to ensure they respect human rights and democratic values. This involves evaluating potential impacts on privacy, non-discrimination, and other fundamental rights. **Implement Human Oversight**: Ensure that AI systems have mechanisms for human oversight to address risks of misuse and ensure compliance with intended purposes. This includes training personnel to monitor and intervene in AI operations as necessary. **Ensure Data Governance**: Develop robust data governance practices to ensure that data used in AI systems is free from bias and respects privacy and
		Article 9 (Risk management system)	This article requires high-risk AI systems to have a risk management system that identifies and mitigates risks to health, safety, and fundamental rights, including privacy and data protection.	
		Article 10 (Data and data governance)	This article mandates that high-risk AI systems use data sets that are free from bias and protect fundamental rights, ensuring fairness and non-discrimination.	
		Article 14 (Human oversight)	This article emphasizes the need for human oversight of high-risk AI systems to prevent risks to health, safety, or fundamental rights, ensuring that AI systems are used in accordance with their intended purpose.	
		Article 27 (Fundamental	This article requires deployers of high-risk AI	

		rights impact assessment)	systems to assess the impact on fundamental rights, ensuring that AI systems respect human rights and democratic values.	data protection laws. This includes regular audits and updates to data sets. **Enhance Transparency**: Maintain transparency in AI operations by clearly informing users when they are interacting with AI systems and providing explanations for AI decisions. This builds trust and accountability.
		Article 50 (Transparency obligations)	This article requires providers and deployers to ensure transparency in AI systems, including informing users when they are interacting with AI, which supports fairness and accountability.	
Transparency and explainability (Principle 1.3)	This principle is about transparency and responsible disclosure around AI systems to ensure that people understand when they are engaging with them and can challenge outcomes.	**Article 10 (Data and Data Governance)**	This article requires that data used in high-risk AI systems be free from bias and that the data governance practices ensure transparency regarding data sources and processing.	**Enhance Transparency**: Businesses should ensure that their AI systems provide clear and understandable information about their capabilities, limitations, and the logic behind their outputs. This includes disclosing when users are interacting with AI systems and marking AI-generated content. **Implement Human Oversight**: Establish mechanisms for human oversight to monitor AI systems and intervene when necessary. This ensures that stakeholders can understand and challenge AI outputs, aligning with the principle of transparency and explainability. **Provide Comprehensive**
		Article 13 (Transparency and Provision of Information to Deployers)	This article mandates that high-risk AI systems be designed to ensure transparency, enabling deployers to interpret the system's output and use it appropriately. It requires that instructions for use include clear and comprehensible information about the AI system's characteristics, capabilities, and limitations.	
		Article 14 (Human Oversight)	This article emphasizes the need for human oversight to prevent risks to health, safety, or fundamental rights. It requires that AI systems be designed to allow effective human oversight, ensuring that stakeholders can understand and	

			challenge AI outputs if necessary.	**Documentation**: Develop detailed documentation for AI systems, including information on data sources, processing methods, and decision-making logic. This helps stakeholders understand the AI system's operations and outputs.
		Article 50 (Transparency Obligations for Providers and Deployers of Certain AI Systems)	This article requires providers and deployers to ensure that AI systems interacting with natural persons disclose that interaction, unless it is obvious. It also mandates marking AI-generated content to indicate its artificial nature, ensuring stakeholders are aware of their interactions with AI systems.	
Robustness, security and safety (Principle 1.4)	AI systems must function in a robust, secure and safe way throughout their lifetimes, and potential risks should be continually assessed and managed.	**Rectial 75**	This recital highlights the importance of technical robustness for high-risk AI systems, emphasizing the need for mechanisms to prevent or minimize harmful behaviour and ensure systems can be safely interrupted if necessary.	**Implement Robust Design and Testing**: Businesses should ensure their AI systems are designed with robust mechanisms to handle errors and adverse conditions. Regular testing and updates should be conducted to maintain system integrity and safety. **Establish a Risk Management System**: Develop a comprehensive risk management system that continuously assesses and mitigates potential risks throughout the AI system's lifecycle. This includes addressing risks from foreseeable misuse and ensuring compliance with safety standards. **Ensure Human Oversight**: Incorporate human oversight mechanisms to
		Article 9 (Risk Management System)	This article requires a continuous risk management process for high-risk AI systems, including regular reviews and updates to address known and foreseeable risks to health, safety, and fundamental rights. It emphasizes the need for measures to mitigate risks that cannot be eliminated through design.	
		Article 14 (Human Oversight)	This article ensures that high-risk AI systems are designed with human oversight capabilities to prevent or minimize risks to health, safety, or fundamental rights. It includes measures to allow human intervention if the	

			system exhibits undesired behaviour.	monitor AI systems and intervene when necessary. This includes training personnel to understand and manage AI operations effectively. **Enhance Cybersecurity Measures**: Implement strong cybersecurity protocols to protect AI systems from unauthorized access and manipulation. This includes measures to detect and respond to potential threats.
		Article 15 (Accuracy, Robustness, and Cybersecurity)	This article mandates that high-risk AI systems be designed to achieve an appropriate level of accuracy, robustness, and cybersecurity throughout their lifecycle. It requires systems to be resilient against errors, faults, and unauthorized alterations, ensuring they function safely under normal and adverse conditions.	
Accountability (Principle 1.5)	Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the OECD's values-based principles for AI.	**Article 9 (Risk Management System)**	This article requires a continuous risk management process for high-risk AI systems, which involves regular reviews and updates to address known and foreseeable risks to health, safety, and fundamental rights. It emphasizes the need for measures to mitigate risks that cannot be eliminated through design.	**Implement a Comprehensive Risk Management System**: Businesses should establish a systematic risk management approach that continuously assesses and mitigates potential risks throughout the AI system's lifecycle. This includes addressing risks related to bias, human rights, safety, and privacy. **Ensure Traceability and Record-keeping**: Develop robust record-keeping practices to ensure traceability of datasets, processes, and decisions made during the AI system lifecycle. This enables analysis of AI outputs and responses to inquiries.
		Article 12 (Record-keeping)	This article mandates that high-risk AI systems allow for automatic recording of events (logs) throughout their lifecycle. This ensures traceability and enables analysis of the AI system's outputs and responses to inquiries.	
		Article 17 (Quality Management System)	This article requires providers of high-risk AI systems to implement a quality management system that ensures	

			compliance with the regulation. This includes maintaining documentation and procedures for regulatory compliance and risk management.	**Maintain a Quality Management System**: Implement a quality management system that includes documentation and procedures for compliance with regulatory requirements. This ensures accountability and proper functioning of AI systems. **Cooperate with Authorities and Stakeholders**: Engage in cooperation with competent authorities and other stakeholders to ensure transparency and accountability in AI operations. This includes providing necessary information and documentation to demonstrate compliance.
		Article 21 (Cooperation with Competent Authorities)	This article obligates providers of high-risk AI systems to provide information and documentation necessary to demonstrate conformity with the requirements, ensuring accountability and transparency.	
		Article 26 (Obligations of Deployers of High-risk AI Systems)	This article outlines the responsibilities of deployers, including ensuring the use of AI systems in accordance with instructions and maintaining logs for traceability. It also requires deployers to monitor AI systems and report any risks or incidents.	

Calls to action

Embed Ethical AI Governance in Business Strategies

Businesses should align their AI development and deployment with the OECD AI Principles, ensuring AI serves human-centric values such as fairness, accountability, and transparency. Establishing internal governance frameworks, ethical AI guidelines, and oversight structures will help companies build responsible AI systems that comply with global standards and foster public trust.

Strengthen AI Transparency and Explainability

Organizations must implement mechanisms to ensure AI decisions are understandable, traceable, and explainable to users and regulators. This includes providing clear documentation on AI models, disclosing when users interact with AI systems, and enabling affected individuals to challenge AI-driven outcomes. Transparency is key to building trust and preventing bias in AI applications.

Implement Robust AI Risk Management and Security Measures

Businesses should proactively assess and mitigate AI-related risks, including biases, cybersecurity threats, and unintended consequences. By integrating continuous monitoring, security audits, and human oversight into AI systems, organizations can enhance AI robustness, reliability, and safety while minimizing harm to individuals and society.

Ensure Accountability and Compliance with AI Regulations

AI actors must be held accountable for the ethical and legal implications of their AI systems. Businesses should implement audit mechanisms, maintain AI system traceability, and cooperate with regulators to demonstrate compliance with evolving AI policies such as the EU AI Act. Establishing accountability structures will help mitigate risks and foster responsible AI adoption.

Conclusion

The OECD AI Principles represent a significant milestone in advancing structured, ethical, and accountable AI governance. As businesses and policymakers navigate the complexities of AI adoption, these principles provide essential guidance for ensuring AI systems are transparent, fair, and aligned with human rights. As a result of emphasizing accountability, inclusivity, and security, the OECD framework is shaping best practices and reinforcing global efforts toward responsible AI development.

However, the real impact of these principles depends on their effective implementation. Organizations face varying levels of preparedness, with challenges such as aligning AI strategies with governance frameworks, ensuring human oversight, and balancing compliance with operational needs. Small and medium enterprises (SMEs) may require additional support to integrate these principles while remaining competitive in a rapidly evolving AI landscape.

Despite these challenges, early adopters are already demonstrating the benefits of structured AI governance. Leading companies across technology, finance, and healthcare are using the OECD AI Principles to enhance transparency, mitigate AI-related risks, and build public trust. By embedding risk management, ethical safeguards, and continuous monitoring into AI systems, these organizations illustrate how proactive governance can drive both regulatory compliance and innovation.

For businesses and policymakers alike, the OECD AI Principles offer a roadmap for responsible AI leadership. Establishing clear governance structures, investing in AI risk assessment, and fostering cross-sector collaboration will be critical in ensuring widespread adoption. As AI continues to shape economies and societies, the principles provide a strong foundation for keeping AI trustworthy, reliable, and aligned with democratic values.

Looking ahead, the long-term success of the OECD AI Principles will depend on continued engagement from industry leaders, refinements in AI governance frameworks, and alignment with emerging regulations such as the EU AI Act. Organizations that proactively adopt these principles will position themselves as global leaders in ethical, effective, and sustainable AI development.

About AI & Partners

AI & Partners

Amsterdam - London - Singapore

AI & Partners – 'AI That You Can Trust'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Contacts

Sean Donald John Musch, CEO/Founder, s.musch@ai-and-partners.com

Michael Charles Borrelli, Director, m.borrelli@ai-and-partners.com

Authors

Sean Donald John Musch, CEO/Founder

Michael Charles Borrelli, Director

References

European Parliament and The Council of the European Union, (2024), 2024/1689 Regulation (EU) 2024/1689 of the European Parliament and of The Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last accessed 15th March 2025)

Organisation for Economic Cooperation and Development, (2025), 'OECD AI Principles overview', accessible at: https://oecd.ai/en/ai-principles (last accessed 15th March 2025)

Important notice

This document has been prepared by AI & Partners B.V. for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of AI & Partners B.V. to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment. Images used throughout the document have either been produced in-house or sourced from publicly available sources (see References for details).

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V