#11 Régulation sectorielle et règlement européen sur l'IA : quelle co-existence?

Co-existence of AI regulation and privacy regulation

Sergi Gálvez Duran
Policy Analyst
Division for Data Flows, Governance and Privacy
OECD

18 November 2024

About the OECD

The Organisation for Economic Co-operation and Development (OECD) is an international organisation in which governments work together to find solutions to common challenges, develop global standards, share experiences and identify best practices to promote better policies for better lives.

Who we are: Our global reach

The OECD brings together **Member countries and partners** that collaborate closely on key global issues at national, regional and local level. Through our standards and initiatives, our work helps drive and anchor reform in **more than 100 economies around the world**, building on our collective wisdom and shared values.

Member Countries	Key Partners	GLOBAL ENGAGEMENT		
		Development Centre	Regional Programmes	Country Programmes
OECD 38 Member countries span the globe	In 2007, the Secretary-General was invited to strengthen OECD co-operation with Brazil, China, India, Indonesia and South Africa through enhanced engagement programmes.	56 countries, of which 27 are OECD members and 29 are developing and emerging economies	Africa, Eurasia, MENA, Latin America and the Caribbean, Southeast Asia and South East Europe	Peru and Kazakhstan completed, Thailand and Morocco underway, Egypt and Viet Nam under discussion

How we work: Our approach

By convening countries and experts, stimulating technical dialogue, and sharing our expertise on social, economic and environmental issues, we help **identify innovative and effective policy solutions**. We do this by:

Inform & advise

As one of the world's largest and most trusted sources of comparative socio-economic data and analysis, we provide knowledge and advise to inform better policies

500+
major reports and country surveys annually

5 billion+
data points annually

Engage & influence

We bring policy makers and policy shapers together to exchange ideas, share experiences and forge progress across a range of policy areas

140,000+
policy makers and shapers visit the OECD annually

300+
committees and working groups underpin our work

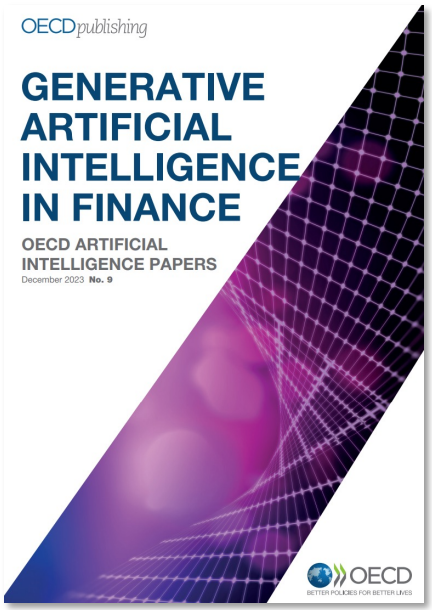
Set standards & provide policy support

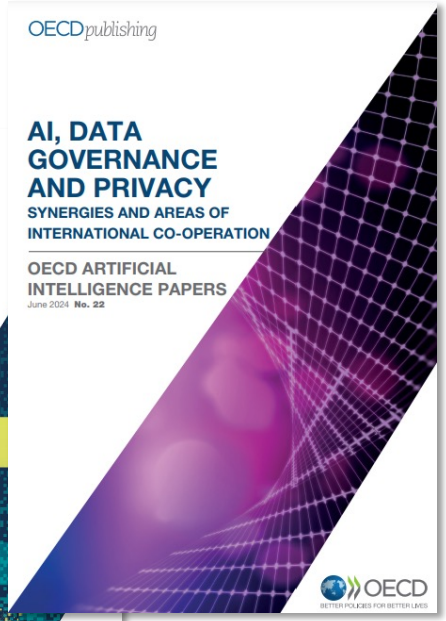
We encourage countries to do better by developing internationally agreed standards so that everyone plays by the same rules and co-operates to reach shared objectives

450+
international standards over the past 60 years

700+
country support projects annually

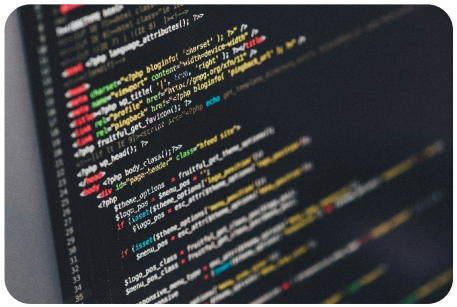
OECD work at the intersection of data, AI and finance



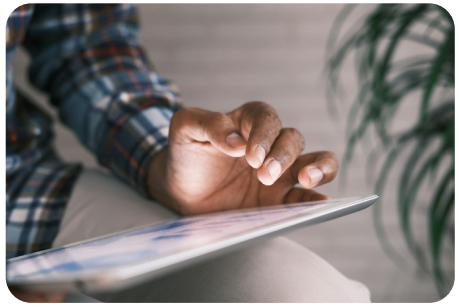


— Structure of this presentation

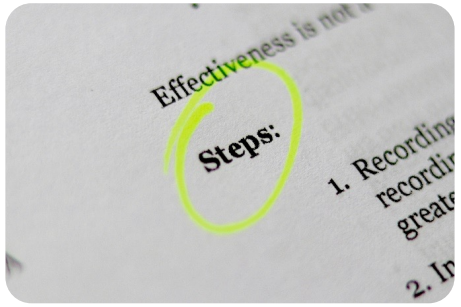
AI's growth and governance



OECD legal instruments on privacy and AI

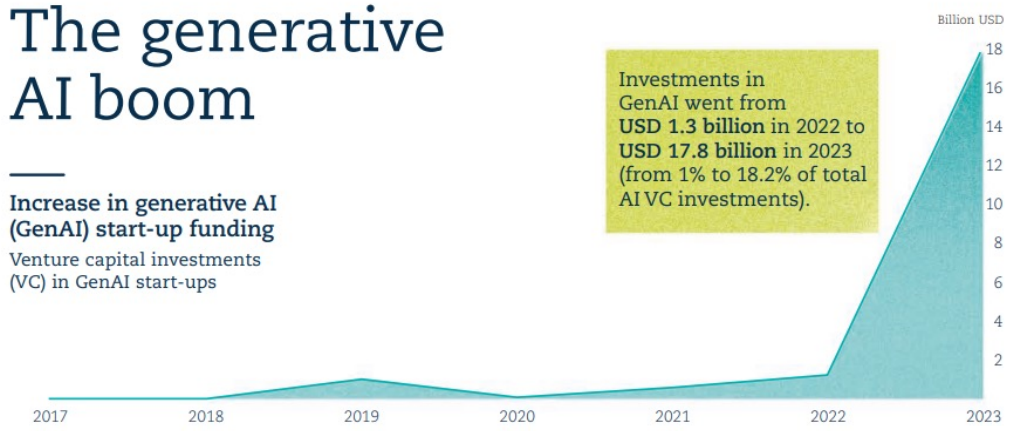


From principles to practice – OECD report on AI, data governance and privacy



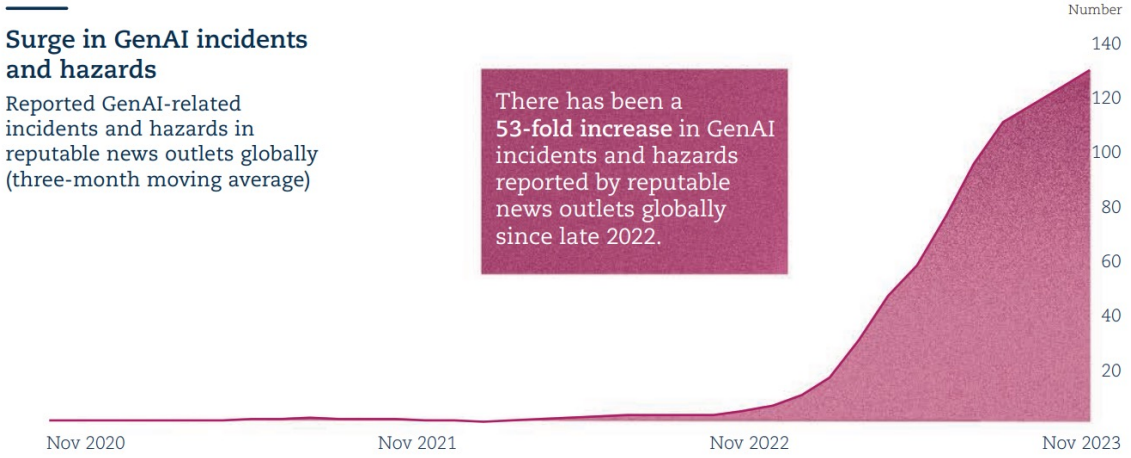
Recent AI advancements have driven exponential growth but also raised questions about trust in the technology

— Exponential growth of AI in recent years

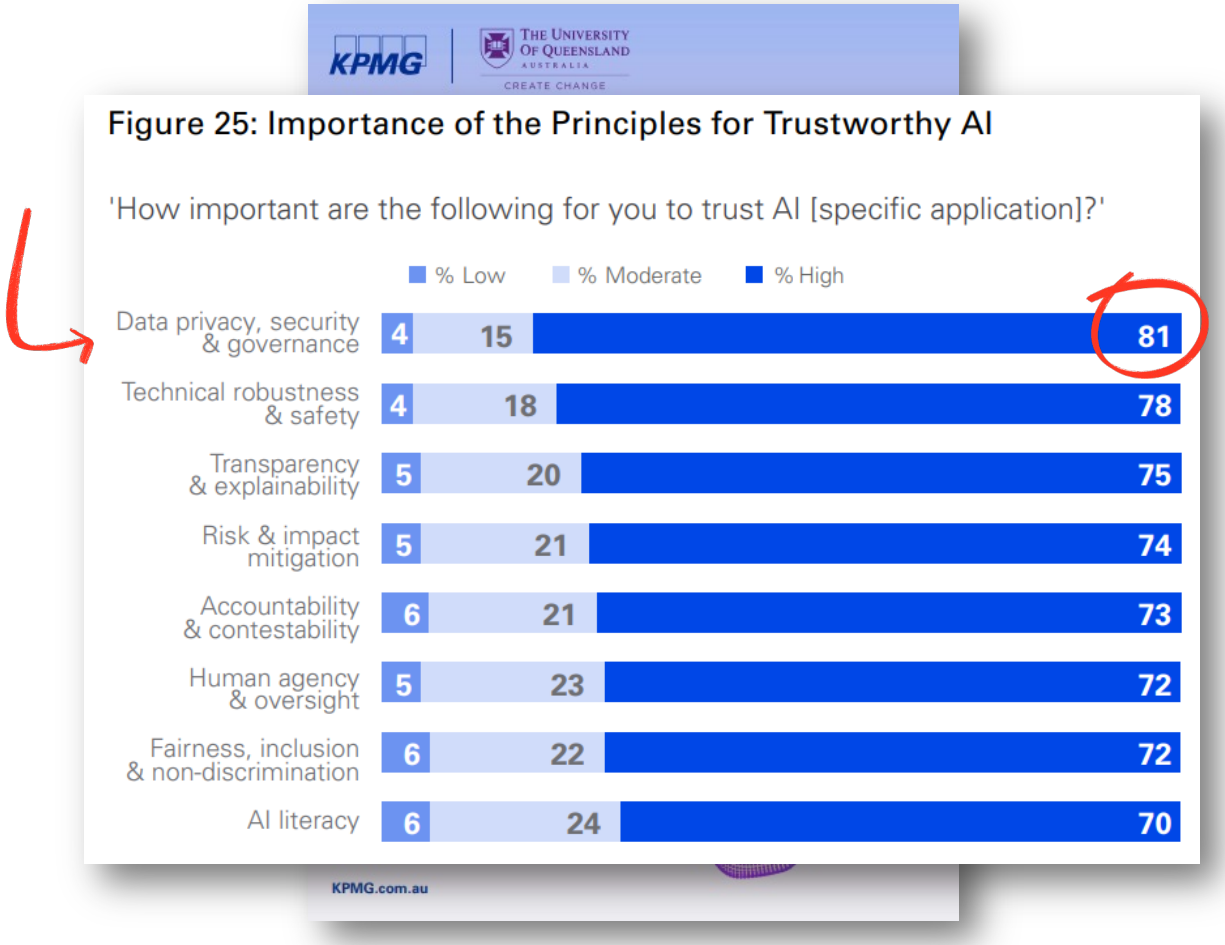


but…

oe.cd/deo2024



Data governance and privacy are key to building trust in AI



OECD legal instruments on privacy and on AI

The Revised OECD AI Principles (2019-2024)

5 values-based principles for trustworthy, human-centric AI


Inclusive growth, sustainable development and well-being


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


Transparency and Explainability


Robustness, Security, and Safety


Accountability

5 recommendations for national policies, for AI ecosystems to benefit societies


Investing in AI research and development


Fostering an inclusive AI-enabling ecosystem


Shaping an enabling interoperable governance and policy environment for AI


Building human capacity and preparing for labour market transformation


International co-operation for trustworthy AI

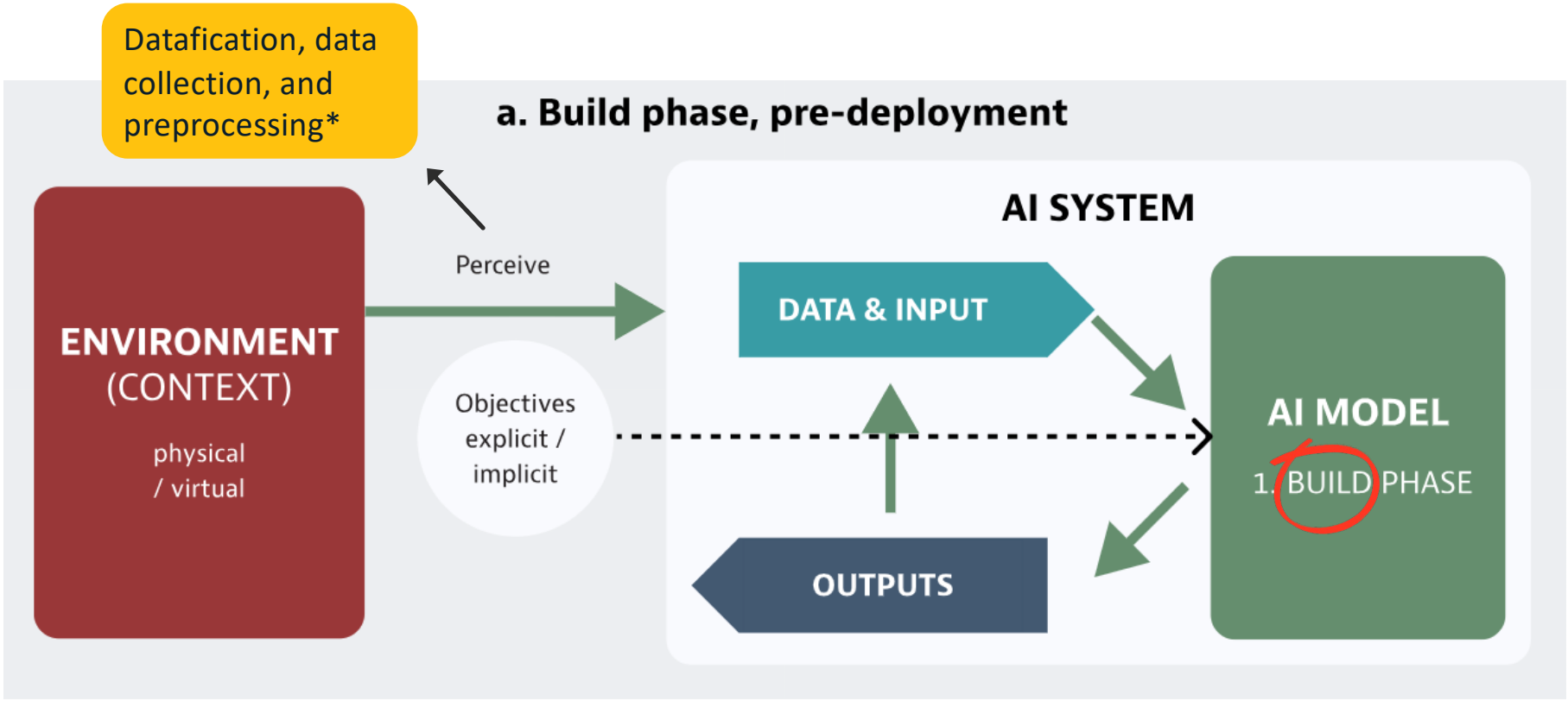
OECD Privacy Guidelines (1980, amended on 2013)

Basic privacy principles

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

These two legal instruments on privacy and AI, combined, provide an **integrated framework** for promoting privacy and data governance across the AI lifecycle

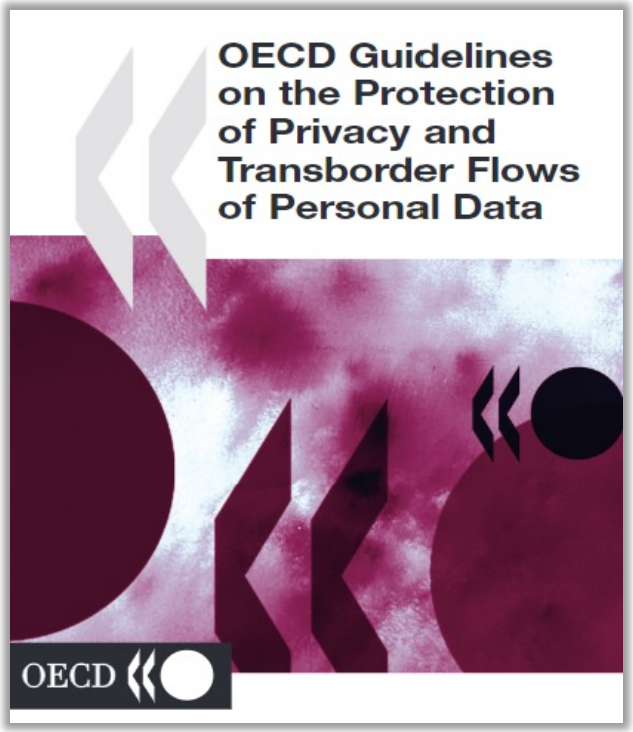
Data/AI lifecycle



Source: Based on OECD (2024), "Explanatory memorandum on the updated OECD definition of an AI system"

* OECD (2015), Data-Driven Innovation: Big Data for Growth and Well-Being

— Build phase, pre-deployment



OECD Privacy Guidelines	
Development of AI systems	Collection Limitation
	Data Quality
	Purpose Specification
	Openness
	Security Safeguards
Deployment for decision-making	Use Limitation
	Access
	Erasure
	Rectification

Challenges in the model building phase

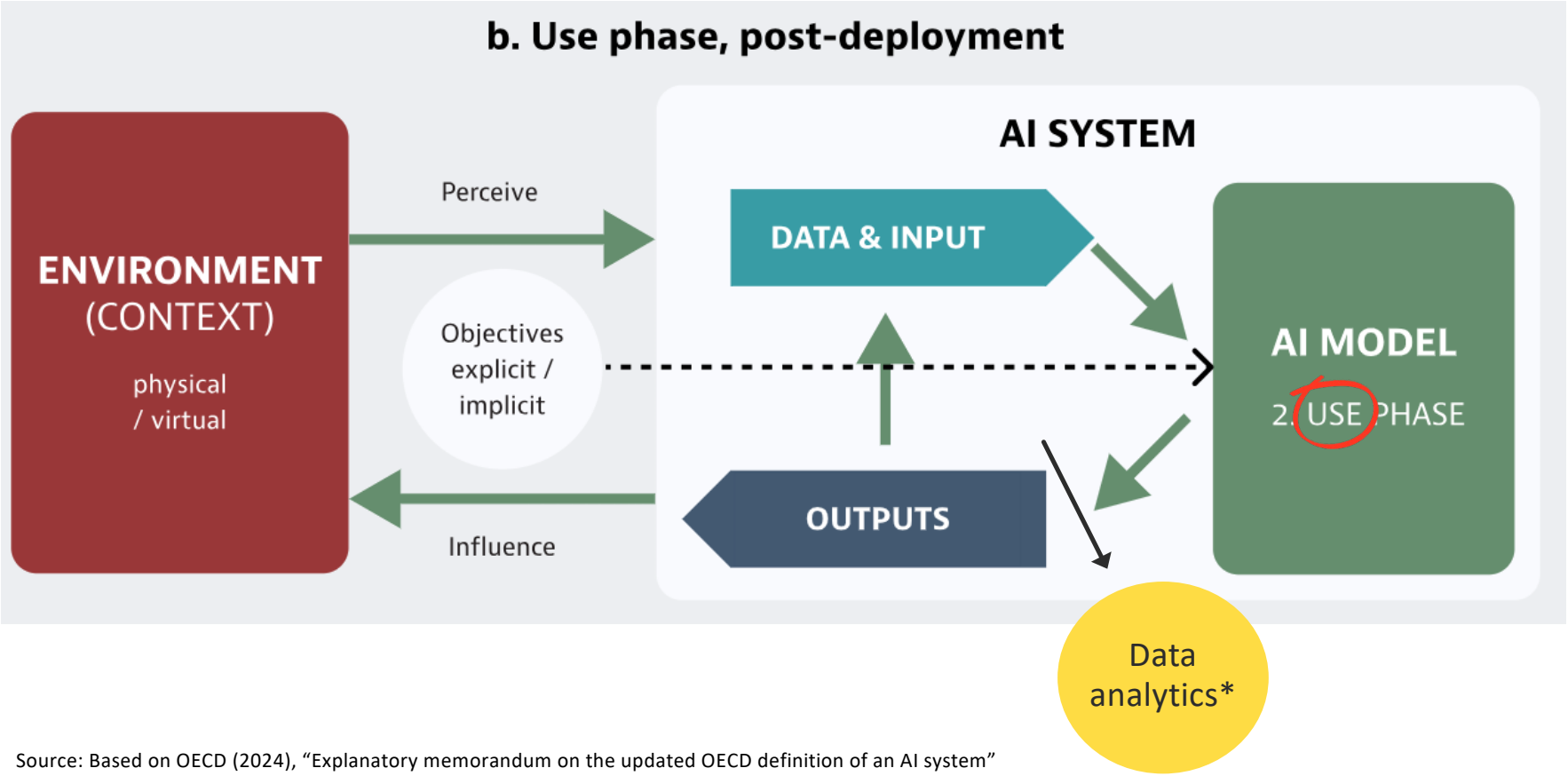
- The **data minimisation** principle is challenged by the nature of AI, which requires large volumes of data to train algorithms

> Should algorithmic accuracy be prioritized? … The EU AI Act allows for the processing of special category data if it is essential to correct discriminatory biases in high-risk systems (art. 10.5)

- AI's ability to discover unexpected patterns in data **makes it difficult to inform individuals in advance** about how their data may be used. Also, the interpretability of deep learning models, functional models, and LLMs remains a challenge

- In certain AI models, such as unsupervised machine learning, it is **difficult to specify the purpose of data processing**, as the algorithm itself determines the future use of the data, not a human

Data/AI lifecycle

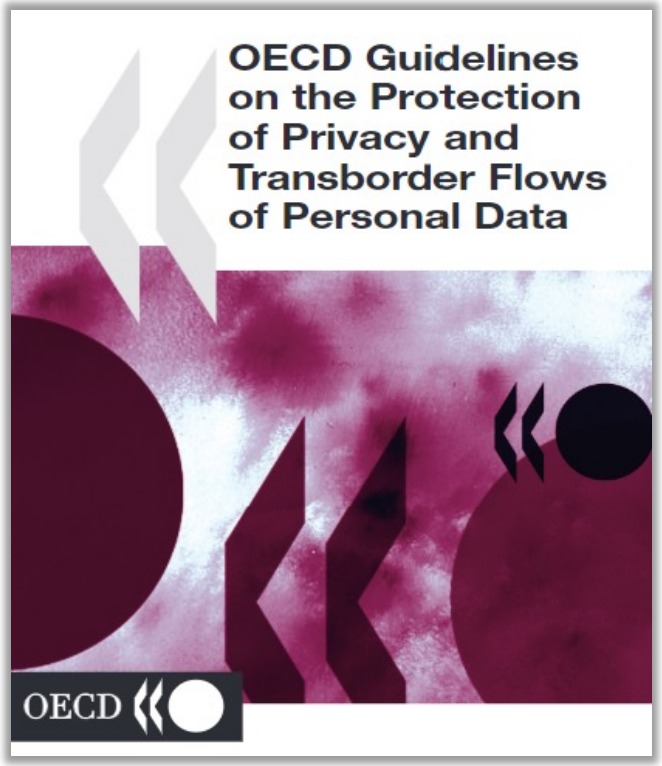


Source: Based on OECD (2024), "Explanatory memorandum on the updated OECD definition of an AI system"

* OECD (2015), Data-Driven Innovation: Big Data for Growth and Well-Being

— Use phase, post-deployment

OECD Privacy Guidelines	
Development of AI systems	Collection Limitation
	Data Quality
	Purpose Specification
	Openness
	Security Safeguards
Deployment for decision-making	Use Limitation
	Access
	Erasure
	Rectification



Challenges in the use phase

- The **possibility of rectification** is essential in the AI context since probabilistic inferences can be inaccurate. However, demonstrating the inaccuracy of algorithmic outcomes is challenging

- AI characteristics make it difficult for individuals to **modify or delete their personal data** and for organisations to provide access to such data

Ensuring these rights in generative AI models is difficult when training data includes unstructured information from the internet. Identifying the specific data point associated with an individual in a dataset can require extensive resources

- **Human review of automated decisions** may be limited by the difficulty of interpreting certain models and by automation bias

From Principles to practice…

Proposals to promote privacy and data governance across the AI lifecycle

Strategic proposals (1/5)

- Privacy and AI policy communities must work together. We need to **understand differences in how terminology is used** between these communities

- Principles and concepts in data privacy and AI need to be mapped to **ensure alignment and to develop a common language** between the communities

Strategic proposals (2/5)

- Collection limitation, purpose specification, use limitation, openness, and data quality principles ensure that AI systems **process personal data fairly and lead to fair outcomes**

- **Risk frameworks** as part of privacy management programmes can help identify and mitigate potential AI system discrimination

Strategic proposals (3/5)

- **Openness principle** is essential to keep individuals informed about use of personal data in both design and deployment of AI systems
- We need new initiatives (e.g., **model cards**) to address the challenge of **AI interpretability** and ensure meaningful information in AI contexts

Strategic proposals (4/5)

- **Embedding safeguards** to protect privacy in AI systems across their lifecycles is essential. **PETs** can help reduce the gap between developing safe AI models and protecting individuals' privacy rights

- We also need new frameworks (e.g., **red-teaming**) to address emerging security vulnerabilities and flaws in AI systems

Strategic proposals (5/5)

- AI actors should consider the potential risks to privacy and data governance **when designing or adopting an AI system**
- **Integration of AI and privacy risk management frameworks** by AI actors is important for addressing data governance risks in AI systems

— Looking ahead

- Continue working with the Expert Group on AI, Data, and Privacy to **deepen the understanding of technological challenges**
- **Encourage collaboration** between regulators and technologists within this group
- Contribute to implementing privacy throughout the AI lifecycle: **upcoming OECD short paper on methods for collecting training data**

Thank you!

dataandprivacy@oecd.org
sergi.galvezduran@oecd.org