

Group Policy Responsible Artificial Intelligence (AI)

AFRY, as an engineering and consulting company in the forefront of innovation, recognize that artificial intelligence (AI) is a transformative technology with the capacity to accelerate AFRY's ambition to unlock transitions. At AFRY, we appreciate that to harness this positive potential sustainably, we must use AI responsibly, carefully consider its social and environmental impacts, and address risks of adverse impacts.

Purpose

The Policy describes the ethical principles and risk management that must apply to the development and use of AI throughout all our operations. It applies to all employees of subsidiaries and entities in which AFRY AB exercises decisive control and extends to contract workers and anyone conducting business on AFRY's behalf. It is supported by the governance and controls outlined in the AFRY Management System and AFRY AI Hub.

References to AI systems in this Policy refers to systems with AI functionality.

Principles

The basic principles of responsible AI include fairness, reliability, trustworthiness, and accountability.

Fairness

People's rights and dignity must always be respected. This means upholding respect for the rule of law and data privacy, and safeguarding against biases, discrimination, and data privacy violations.

Reliability

AI systems must be robust, resilient, safe, and quality assured. Risks must undergo documented risk assessments prior to deployment and be managed throughout the AI system life cycle.

Trustworthiness

The purpose and functioning of AI systems must be transparent and their organizational and technical

safeguards adequately documented to enable testing and monitoring.

Accountability

Humans remain responsible for decisions supported by AI. This means that we must understand our personal accountability for assessing and minimizing risks, including ensuring we have adequate training and competence commensurate with the risks associated with our use of AI.

Risk Management

Given the rapid development of AI capabilities, effective governance relies on meaningful stakeholder engagement, dialogue, knowledge sharing, continuous training, guidance, and a high level of risk awareness.

The AI functionality must be classified according to defined risk tiers, with governance and control requirements proportionate to the level of risk posed by the AI functionality. Detailed criteria and procedures for risk classification are set out in the guidance maintained by the AFRY AI Hub hosted at Group IT (hereinafter "AI Hub").

Risk management must be incorporated throughout AI systems' life cycle, with adequate assessments at all stages including planning, design, data collection and processing, development, adaptation, deployment, operation, and retirement. The risk management must be verified by monitoring and periodic testing. The risk assessments and safety documentation must be sufficiently complete and transparent to enable audit.

When procuring systems that embed AI from third-party providers, due diligence must be conducted to ensure the system meets AFRY's safety, privacy, and ethical standards. The scope and depth of such due diligence shall be proportionate to the significance and risk of AI functionality within the system.

Acceptable Use

The use of AI must comply with all applicable laws, regulations, internal policies, and contractual commitments, including those relating to data privacy and protection, intellectual property rights, and confidentiality. All employees must protect both AFRY's proprietary information and the information of AFRY's clients and other stakeholders. The use of AI for any unlawful, unethical, or unauthorized purpose is strictly prohibited.

Employees must exercise their professional judgment. At a minimum:

- Verify and take ownership of any output that includes or relies on AI-generated content.
- Consider the limitations of AI and cross-reference AI-generated content with reliable sources before using it for critical decisions and in customer deliveries.
- Remain vigilant to potential biases in AI-generated outputs.
- Be transparent regarding the use of AI in your deliveries.
- Complete required training and maintain awareness of the capabilities, limitations, and risks of the AI systems you use.
- Employees, when in doubt, must seek guidance about the appropriateness of a particular AI application.

To facilitate uptake, AFRY has pre-approved several external AI systems that meet AFRY's data security standards (i.e., AFRY-approved tools) and made these available to AFRY employees. Any other external AI systems must be reviewed via the AI Hub before use. Approval requests must be submitted through the AI Hub.

Roles and responsibilities

The AI Hub maintains guidance and risk classification criteria, supports risk assessments, and reviews due diligence on third-party AI systems. The AI Hub also provides guidance on external AI systems not pre-approved by AFRY as well as strategic oversight of AI governance.

Group IT is responsible for due diligence in AI systems that are procured.

The Chief Ethics & Compliance Officer owns this policy and is responsible for its periodic review.

Enforcement

Any individual with access to AFRY's environment who intentionally or negligently fails to comply with this Policy may be subject to disciplinary action.

Frameworks

This Policy is informed by, and intended to align with, applicable regulatory frameworks and international guidance on artificial intelligence, including the European Union Artificial Intelligence Act (EU AI Act) and the Organization for Economic Co-operation and Development (OECD) Due Diligence Guidance for Responsible AI. These instruments establish foundational principles for the responsible development and deployment of AI systems. As the regulatory landscape continues to evolve, this Policy and its supporting guidance will be reviewed and updated to ensure continued alignment with applicable legal and regulatory requirements.