

Responsible Artificial Intelligence Program in Hera Group

Solid infrastructures for a long-term sustainable strategy

Photo by Silvia Camporesi: construction phase of the biomethane plant of Sant'Agata Bolognese



Governance and controlled access to sensitive AI capabilities

Control does not start from the individual tool, but it starts from risk classification, data governance, cybersecurity and clear accountabilities:

AI classification and “need-to-use” principle:

- Mapping of AI use cases by risk and criticality
- Limited access to high-impact capabilities, with dedicated authorizations
- Prohibition/enhanced control for facial recognition, surveillance or invasive uses

Controls on data and platforms:

- Group data strategy focused on quality, reliability and accountability
- Cloud/collaboration platforms with structured adoption programmes
- IT/OT cybersecurity and vulnerability assessments, including for plants

Alignment with the AI Act:

- Risk-based approach for providers and users of AI systems
- Integration of technology, legal, data governance and compliance expertise
- Human oversight for the most sensitive use cases

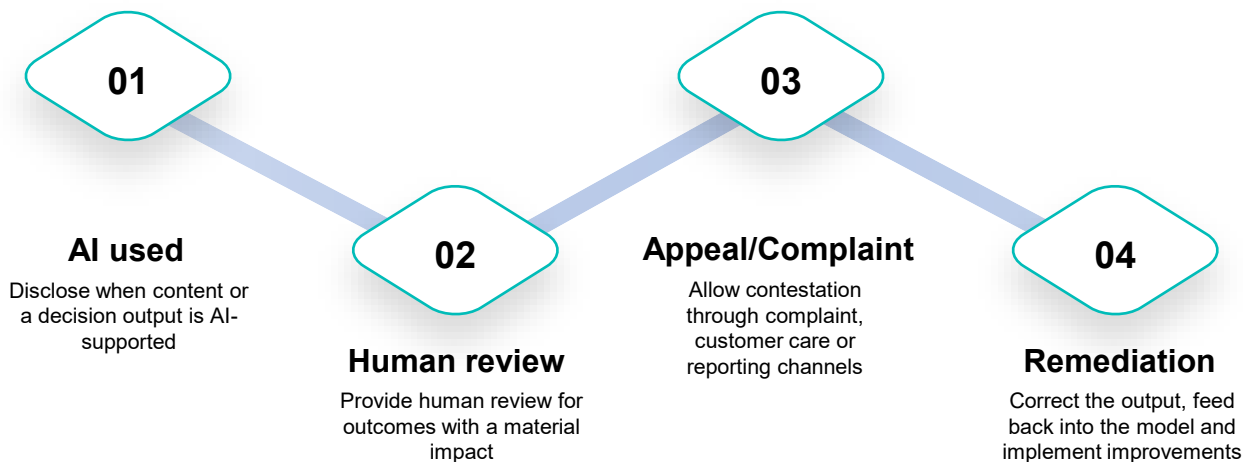
Ethical accountability:

- Code of Ethics as framework for conduct and responsibility
- 2026 update with stronger focus on digital transition and AI
- Ethics and Sustainability Committee for reports and improvements

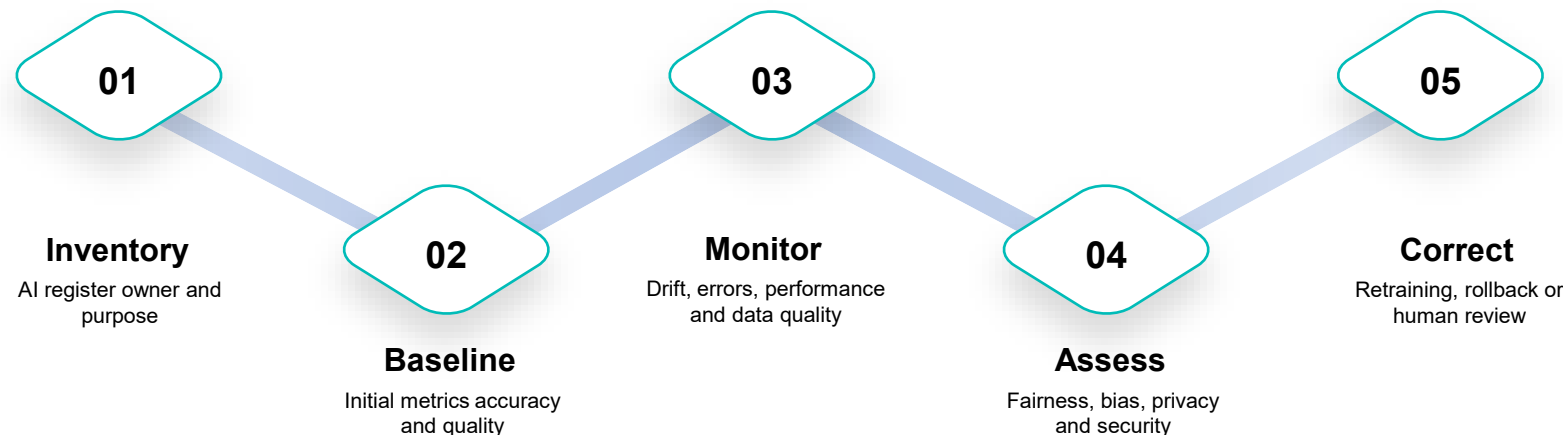
*Transparency,
labelling and
ability to
contest an AI
outcome*

*Model
monitoring, drift
and
fairness/bias*

For cases affecting customers, employees or third parties, Hera can connect AI governance to existing communication, complaint and dialogue safeguards with this guidelines and procedures:



The objective is to turn each AI model into a controlled asset: owner, KPIs, thresholds, audit trail, periodic testing and remediation plan.



Minimum controls in place

- Alert thresholds on accuracy, false positives/negatives and data quality
- Periodic testing for protected categories or sensitive proxies, where applicable
- Audit logs, functional owner, technical owner and change approval
- Incident/remediation playbook and review after complaints or anomalies



AI ecological footprint and measurement of sustainability impacts

Hera can frame AI not as an end in itself, but as a lever for service quality, circular economy, resilience and impact reduction:

Operational impact:

- Potential improvements in quality, costs and targeted information campaigns

CSV measurement:

- Shared-value EBITDA and CSV investments as impact proxies
- Environmental KPIs for carbon neutrality, resource regeneration and resilience

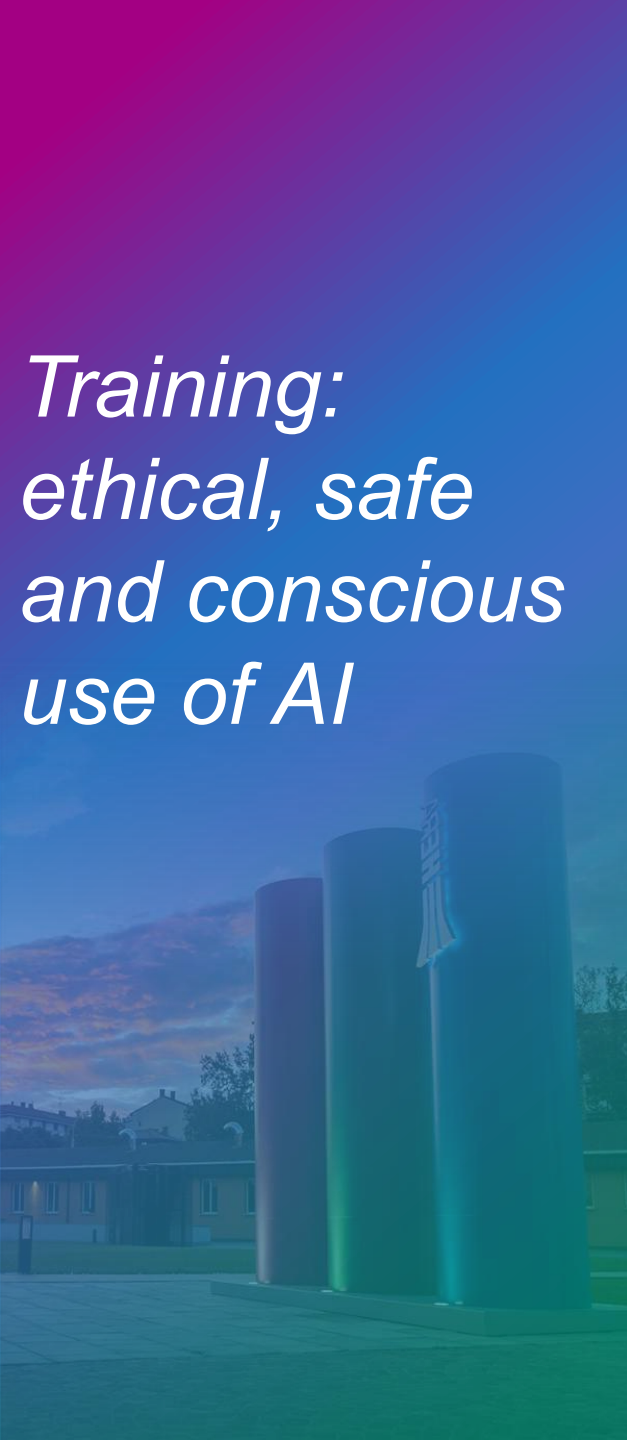
Digital footprint:

- Cloud/data centres with security, privacy, efficiency and sustainability standards
- Supplier choices and architectures aligned with energy performance and scalability

AI impact reporting:

- Ex ante/ex post KPIs for each use case
- Energy consumed, operational savings, avoided emissions, service quality and stakeholder benefits

Thanks to its presence in the data center business through its subsidiary HeraBit, Hera is reducing the carbon footprint of its data centers and is designing a new one to meet the highest energy standards.



Training: ethical, safe and conscious use of AI

Training is the bridge between technology and responsibility: guided GenAI adoption, cyber awareness and data culture:

AI adoption programme:

- Structured pathways from familiarisation to operational best practices
- Bottom-up identification of new AI use cases
- Focus on drafting, summarisation, knowledge management and communication standardisation

Cybersecurity training:

- Awareness of threats and correct behaviours
- Ethical phishing simulations
- Improved user defences and reporting channels

Data culture:

- Training programs linked to the data strategy
- Managing data as a strategic asset
- Ethical and responsible interpretation of information

Examples of training content:

- Data classification and ban on entering confidential data into unauthorised tools
- Safe prompting, source verification and hallucination management
- Bias, fairness, inclusion and human oversight
- Labelling of AI-generated content and user accountability
- Security by design, privacy, intellectual property and protection of information