

**POLICY ON THE RESPONSIBLE USE OF ARTIFICIAL
INTELLIGENCE OF MERLIN PROPERTIES, SOCIMI, S.A.**



December 2025



The Board of Directors of MERLIN Properties, SOCIMI, S.A. (hereinafter "**MERLIN**", the "**Group**" or the "**Company**") has approved this Policy on the Responsible Use of Artificial Intelligence (hereinafter, also the "**Policy**" and, where applicable, "**AI**"), following a report from the **Appointments and Remuneration Committee** and at the proposal of the **Sustainability and Innovation Committee**, which establishes the basic principles of action that must govern the design, development and application of artificial intelligence tools in accordance with the regulations applicable at all times and with their ethical values, defined in the **Code of Conduct**, as well as with the provisions of other applicable internal regulations.

Likewise, **this Policy is understood to protect and safeguard users' information, systems and privacy, as well as to comply with current regulations** (in particular, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized standards in the field of 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 (the European Artificial Intelligence Regulation or RIA).

1. General aspects and scope of action

The development and implementation of artificial intelligence tools is an essential element for value creation, as well as for the Group's innovation and digital transformation strategy. For this reason, the Group's Board of Directors recognizes the importance of promoting its responsible use, in accordance with the principles that make up its corporate culture, based on ethics and commitment to sustainability.

An Artificial Intelligence System is understood as one that is automated and that is designed to operate with different levels of autonomy and that can show the ability to adapt after deployment, and that, for explicit or implicit objectives, infers from the input information it receives the way to generate output results. such as predictions, content, recommendations or decisions, which can influence physical or virtual environments.

MERLIN will use AI systems in a responsible, transparent, secure and reliable manner. To this end, it assumes and promotes basic principles of action that must preside over its activities related to the design, development, application and use of artificial intelligence tools at work in a safe and innovative way and creative and effective.

This Policy is understood to be framed within the **Information Security Management System** (also known as "**ISMS**"), in accordance with and based on the international standard ISO 27.001 in accordance with the **Information Security Policy**, as well as other applicable related regulations.

The Information Security Management System preserves the confidentiality, integrity and availability of information by implementing a risk management process and gives confidence to stakeholders that risks are properly managed.



This Policy is applicable to all employees, managers and directors of all the companies that make up the Group, including those investee companies over which it has effective control, within the limits provided for in the applicable regulations.

In these companies in which the Group does not have effective control, the representatives of MERLIN, within the scope of their possibilities, shall propose principles and guidelines consistent with those established in this Policy.

The application of the Policy may be extended, in whole or in part, to any other natural and/or legal person linked to the Group by a relationship other than employment when this is possible due to the nature of the relationship and is convenient for the fulfilment of the purpose of the same.

In accordance with the Policy, MERLIN may develop procedures to implement and comply with the obligations assumed, as well as to adapt it to the various legislations applicable to the Group.

Likewise, the application of **this Policy is complementary to other mandatory internal regulations**, such as:

- The Code of Conduct
- The Information Security Policy
- Internal Regulations for the use of Artificial Intelligence
- Manual for the use of Information Systems and Personal Data.
- The Personal Data Protection Policy.

2. Objectives of the Policy

The purpose of this **Policy** is to establish the basic principles of action that must govern the application of artificial intelligence tools, understood as any automated system designed to operate with different levels of autonomy and that can, with explicit or implicit objectives, generate results such as predictions, recommendations or decisions, which in turn influence physical or virtual environments.

This Policy constitutes the **reference framework** by which MERLIN defines the guidelines for the use of Artificial Intelligence systems by the Group:

- **Guaranteeing its responsible use.** Artificial intelligence systems will be developed and used as tools at the service of people, with full respect for people's fundamental rights.
- **Maintaining traceability and transparency**, ensuring that users are aware that they are communicating or interacting with an artificial intelligence system.
- **In a safe and reliable way**, ensuring that artificial intelligence systems are used in a way that minimizes unintentional damage and is resilient against illicit use by malicious third parties, always ensuring business continuity.



3. Fundamental principles of the Policy

In pursuit of the above, Merlin's fundamental principles of express commitment are the following:

- **Security:** Protect data, processes, and outcomes from external actors, adverse events, and misinformation. This requires the implementation of robust measures and processes that include cybersecurity policies, encryption, access controls, and regular audits, among other controls.
- **Protection:** Protect the fundamental rights, health and safety of the people, as well as companies and their property from possible damage. This includes identifying, assessing, and mitigating risks throughout the system's lifecycle, from initial development to deployment and operation.
- **Privacy:** To process personal data on a legitimate basis, with the prior implementation of technical and organizational measures that protect the confidentiality, integrity and availability of personal data, as well as to guarantee respect for the rights of data subjects.
- **Ethical application:** Require ethical and social assessments to be carried out before initiating any AI project, identifying possible negative impacts on employees, customers and other stakeholders. These assessments should include reviews of algorithmic biases, fairness in decision-making, and respect for digital rights.
- **Ensure human oversight:** Designated decision-makers should have the power to review, modify, or override any critical decisions made by AI systems, especially those that affect essential rights of employees, customers, or third parties.
- **Equity:** ensuring that AI systems are developed and/or used in a way that promotes equal access, gender equality and cultural diversity, while avoiding discriminatory effects and unfair bias. Fairness in AI not only involves eradicating biases in the data used for training but also promoting transparency in the algorithms and processes that systems employ to make decisions.
- **Transparency:** Users and stakeholders must understand how AI systems work and the process by which decisions that affect them are made. This includes providing clear and accessible information about the use of personal data, processing processes, and the rights you can exercise in relation to such systems.
- **Traceability:** Ensuring that AI systems are understandable as to how and why they make their decisions. This means that the system's internal processes, algorithms and models are clear and can be translated into documented explanations that are understandable to the people concerned, such as employees and users.
- **Responsibility:** Establish a clear framework of accountability throughout the system's lifecycle. This implies that each party involved, from developers, including their management staff, to end users, has specific roles and assumes responsibility for their actions and decisions regarding these systems.



- **Reliability:** Ensuring that the system operates consistently and predictably in different conditions and scenarios. A reliable system must demonstrate stability, accuracy, and resistance to failure, ensuring that its results are reproducible and aligned with the intended objectives.
- **Respect Intellectual Property:** Ensure that the use of artificial intelligence respects the intellectual and industrial property rights and trade secrets of third parties during the training, validation and testing phases (inputs), as well as in the generation of results (outputs).
- **Data integrity:** Ensure the fidelity and integrity of the datasets used at all stages of the AI system's lifecycle (conception and analysis, development, operation, and/or removal of the treatment/component).

4. Governance in the use of Artificial Intelligence

To ensure the correct implementation of this Policy, MERLIN considers it essential to establish clear roles and responsibilities for both supervision and implementation.

The body responsible for governance is the **Board of Directors**, as the Group's highest decision-making body, which has set up the Sustainability and Innovation Committee, as a permanent internal body, of an informative and consultative nature, without executive functions, with powers of advice, information and proposals on technological risks.

The **Sustainability and Innovation Committee** is responsible for promoting innovation, especially in relation to digitalization and technology, for the sustainable evolution of the Company and its group, making proposals to the Board of Directors on action plans and their implementation, in coordination and consultation with the executive team.

For its part, the **Management Team** of MERLIN Properties is responsible for the transfer and integration of the guidelines and commitments contained in this policy in the decision-making and daily management of the company's activities. The management team is also responsible for the allocation of resources to comply with the commitments made in this policy.

On the other hand, the **Information Security Committee** made up of the CEO, CTO, CIO and other members of the Management aims to ensure that good practice on the use of Artificial Intelligence tools is applied effectively and consistently throughout the Group.

The **Information Security Officer (CISO)** will exercise their control function independently, and it is their responsibility to implement this policy and monitor its compliance, as well as that of all the requirements derived from the applicable laws, regulations and good practices in the field of Information Security.

The **Personal Data Protection Officer (DPO)** will independently supervise the processing of personal data, in each of the phases of the life cycle of AI systems, complies with applicable data protection regulations, including the GDPR and the LOPDGDD, as well as evaluate and mitigate the impact on user privacy derived from the use of Artificial Intelligence tools.



The **head of Human Resources** will define the transformation and digitalization capabilities of Merlin's staff and develop the literacy plan in the use of AI tools required by the regulation.

Finally, all Group **Employees** must know, assume and comply with the Policy, as well as the internal regulations on security and use of the systems in force, being obliged to maintain professional secrecy and confidentiality of the information handled in their work environment and must communicate, as a matter of urgency and in accordance with the established procedures, any possible incidents or security problems that are detected.

5. Control and auditing

MERLIN expressly reserves the right to adopt, in a proportional manner, the necessary surveillance and control measures to verify the correct use of the Systems it makes available to its employees, including the content of communications and devices, respecting, in all cases, the legislation in force and guaranteeing the dignity of the employee. The communication of this Policy will have the effect of prior notification to the worker.

Likewise, MERLIN will ensure the correct use of artificial intelligence systems by external collaborators in the services they provide to the different companies of the Group.

The Group will undergo periodic reviews and controls, as well as internal and external audits, to assess overall compliance with this Policy.

6. Policy Communication

This Policy will be available to all employees and will be available to all the Company's stakeholders on the corporate website. Likewise, the Policy will be subject to appropriate communication, training and awareness-raising actions for its timely understanding and implementation.

7. Policy Update and Review

This Information Security Policy has been approved by the Board of Directors of MERLIN Properties in december 2025, entering into force at the time of its approval and being fully in force as long as there are no modifications to it.

The Board of Directors, through its Executive Committees, and particularly through its Sustainability and Innovation Committee and the Information Security Committee, will supervise the correct implementation and compliance with all the principles of action and commitments set out.

In the event of this, the modifications made to the Policy on the Use of Artificial Intelligence Systems will be applicable from the day following their communication to all stakeholders affected by this Policy.