konecta

Artificial intelligence management and governance policy

Corporate Policies 2025

Table of contents

Before printing this document, be sure it is necessary. It is in our hands to protect the environment.

01

Introduction

This document has been drawn up to ensure compliance with current regulations on artificial intelligence by all entities that make up the Konecta business group, as well as to enable all interested parties or stakeholders to follow the recommendations issued by the relevant bodies in this area.

The purpose of this Artificial Intelligence Management and Governance Policy (hereinafter, the "Policy") is to ensure the ethical, responsible and secure adoption of Artificial Intelligence technologies (hereinafter, "AI") within Konecta, a multinational group of companies specialising in the provision of digital customer management services and solutions (hereinafter "Konecta").

To this end, a robust governance framework is established to identify, assess and mitigate the risks that may arise from the introduction onto the market, commissioning, use and, where applicable, decommissioning of AI Systems (as defined in this Policy). This Policy is designed to protect public interests, safety and health, as well as the fundamental rights recognised by the legal system applicable to Konecta and the territories in which it operates[1].

Definition and scope

AI represents a strategic technology for Konecta's digital transformation. However, its development and adoption require ensuring an appropriate balance between innovation and control, in accordance with corporate ethical values and the current regulatory framework.

In this context, this Policy has been developed with the aim of establishing an internal and cross-cutting regulatory framework for the use of AI systems (both generative and non-generative), adopting a risk-based approach[2].

For the purposes of this Policy, the following definitions shall apply:

- "Algorithm": mathematical logic that enables the creation of models that can make predictions, classify data, recognise patterns and even make decisions.
- "Use Case": combination of technologies that use AI to solve a specific problem within Konecta or linked to AI systems designed for a specific purpose and aimed at a specific group of users, with access to a specific type of information. Use Cases may integrate one or more AI models as part of the functionality of the AI system.
- "Distributor": any person or company that is part of the supply chain and sells an AI System, other than the supplier or importer.
- "Artificial Intelligence Tools" ("AIT"): software applications or platforms that use AI and machine learning techniques to perform specific tasks or solve particular problems.
- "Importer": any person or entity that introduces an AI system into the market that bears the name or brand of a person or company from another country.

[1] Recital 5, AI Regulation (Regulation (EU) 2024/1689 on Artificial Intelligence.

[2] The approach adopted by the Regulation establishes a common risk-based framework and imposes obligations on all actors in the AI value chain, from suppliers to those responsible for deployment, with significant penalties for non-compliance.

- “Inputs”: data, content or information that is fed into an AIT for training and processing. This may include text, images, numbers or any other type of information that the AIT can use.

- “General-purpose AI model” (“AI model”): an AI model, including one trained with a large volume of data using large-scale self-supervision, that exhibits a considerable degree of generality and is capable of competently performing a wide variety of different tasks, regardless of how the model is introduced to the market, and which can be integrated into various downstream systems or applications, except for AI models used for research, development, or prototyping activities prior to their introduction to the market. General-purpose AI models are integrated into AI Systems, but are not systems themselves.

- “Outputs”: these are the results or information generated by an AI system after processing the inputs. This can take various forms such as text, graphics, decisions or recommendations, depending on the function of the AIT.

- “Supplier”: any person or entity that creates an AI System. This Supplier may be a company, a public organisation, or even an individual. The Supplier places the AI System on the market or uses it under its own name or brand, either for a fee or free of charge.

- “Regulation”: 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.

- “Authorised representative”: any person or entity that has been authorised in writing by an AI Provider to fulfil obligations and procedures on its behalf.

- “Deployment manager” or “deployer”: any person, company or organisation that uses an AI system under its own responsibility. This does not include the use of AI for personal activities that are not professional.

- “Bias” in AI: any systematic tendency or inclination that appears in the results generated by an AI system, which may be based on biased data, incorrect assumptions, or prejudiced algorithms. This bias can lead to unfair or inaccurate decisions when applied to different groups of people or situations.

- “Artificial Intelligence System” (“AI System”): a system based on machines containing data, algorithms and models, designed to operate with varying levels of autonomy and capable of demonstrating adaptability after deployment, which, for explicit or implicit purposes, infers from the inputs it receives how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments. (Software systems with capabilities below those specified above are excluded, such as traditional and simpler software systems or programming approaches, and do not include systems based on rules defined solely by natural persons to automatically execute operations).

- “Automated decisions”: decision-making by technological means without human involvement.

- “Traceability”: the ability to track and document how an AIT reaches a specific conclusion or generates certain results. This includes understanding and documenting input data, algorithms, processes, and any other factors that influence the results. Traceability is crucial to ensuring transparency and determining accountability in the use of AITs.
- “Transparency”: is the degree to which the processes and decisions made by an AIT are clear, understandable, and explainable to users and other stakeholders.
- “User”: is any person, whether employed or not, who has a professional or contractual relationship with Konecta and uses AIT to interact with it. The User may be either internal (an employee) or external (a customer, supervisor or supplier).
- “Monitoring mechanisms”: systematic process of examining and evaluating (auditing) the methodology, operations and results of an AIT to ensure that it complies with Konecta's ethical, legal and organisational standards. Monitoring mechanisms are crucial for identifying risks and biases and ensuring accountability and transparency.

As a signatory to the United Nations Global Compact, which it joined in 2004, Konecta is committed to Principles 1 and 2, which focus on respect for and non-violation of human rights, considering privacy and data protection to be a fundamental human right in the digital age. Likewise, in order to contribute to the agenda set by the United Nations for sustainable development, the company has adopted the Sustainable Development Goals within the framework of the 2030 Agenda.

02

Scope of application

This corporate policy falls within the scope of the Compliance Framework Policy and shall apply to all companies that form part of Grupo Konecta. It is endorsed by the company's senior management and constitutes an internal regulatory framework for the responsible management and application of both generative and non-generative AI.

In accordance with the above, this Policy shall apply to all interested parties (employees, suppliers, contractors, consultants, temporary staff and third parties) operating within the environment of the Companies that form part of Konecta, without prejudice to compliance with other regulations and internal documents in force, and must be interpreted in harmony with the sectoral, territorial and extraterritorial regulations applicable at any given time to the various entities that make up Konecta, as well as with other internal documentation related to this matter, such as, for example, the Procedure for Responsible Management and Implementation of AI.

In particular, this Policy defines the minimum requirements that AI-based Use Cases must meet, depending on the level of risk they present.

Compliance with this Policy does not exempt, in any case, from compliance with other internal or external regulations, such as Konecta's Responsible AI Management and Implementation Procedure and/or any others that may be applicable to each Use Case, such as those relating to the protection of personal data, intellectual and industrial property, confidentiality of trade secrets, cybersecurity or other sectoral or cross-cutting regulatory obligations.

Konecta entities must transpose its principles and requirements into their respective internal regulations, and are responsible for their development, interpretation and compliance. To this end, they must approve (in their corresponding governing bodies) the internal regulations that enable the application of this Policy.

This Policy shall apply in all countries in which Konecta operates, regardless of the degree of local regulatory development in the field of AI.

Likewise, in territories where there is still no specific regulation on AI, this Policy will serve as a minimum standard of conduct. When a country adopts regulations on AI, the application of this Policy will be conditional upon it not contradicting those local regulations. In the event of a discrepancy between regulations, the strictest provision or the one that best protects fundamental rights, safety or public interests will always prevail.

Management Commitment

Konecta's senior management, understanding the importance of proper AI management throughout its life cycle and in accordance with the company's strategic planning, is committed to:

- AI management model.
- Ensure that the necessary resources are available for the proper functioning of the AI System.
- Achievement of the organisation's objectives in the field of AI.

- Ensure AI management processes and the reliability of AI systems, as well as the protection, security, fairness, transparency, data quality, and quality of AI systems throughout their lifecycle.

- Compliance with all applicable legal, regulatory, and contractual requirements.

- Inform, train and raise awareness among all stakeholders of their roles, obligations and duties in relation to AI.

- Reduce the risks associated with AI aspects through a process of analysis, assessment and treatment of these risks.

- Continuously improve the AI management model.

- The appointment, actions and decisions taken by the Data Governance and Quality Forum.

- Ensure the availability and accessibility of this Policy to all interested parties.

03

Guiding principles applicable to use cases

In order to ensure an ethical, secure and legally robust framework for the use of AI, Konecta promotes the application of the following fundamental principles throughout the entire life cycle of AI-based use cases.

Privacy and security

Konecta is committed to ensuring that the design, development and use of its AI Systems comply with the highest standards of privacy and personal data protection. This principle also includes the adoption of appropriate cybersecurity measures to prevent misuse, loss, alteration or unauthorised access to the information of customers, employees and other stakeholders.

Positive impact

Konecta uses AI as a tool to generate social and economic value, offering products and services tailored to the needs of its stakeholders. In this regard, it will actively promote AI systems that contribute to the general well-being and sustainable development of the communities in which the entities that make up Konecta operate.

Equality and inclusion

Konecta designs and applies its AI systems under the principles of fairness, non-discrimination and inclusion. Specific measures will be implemented to identify and mitigate potential algorithmic biases, ensuring that the results of the systems are impartial and respectful of the fundamental rights of all individuals, especially in sensitive or high-impact contexts.

Observability, supervision and transparency

All use cases shall include monitoring, verification, and moderation mechanisms to validate that the AI system meets the objectives for which it was designed. Likewise, clear, accessible, and understandable information shall be provided to customers, employees, auditors, and regulators on the operation and purpose of such systems.

Technical and contextual robustness

The AI systems implemented by Konecta will be robust not only from a technical point of view, but also in terms of their suitability for the social, legal and organisational environment. Use cases must minimise errors, prevent unintended damage and be resilient in the face of failures or adverse scenarios.

Transparency and explainability

Konecta will adequately inform Users when they interact with Konecta's AI Systems. Additionally, it will ensure that such Users can understand, in simple terms, the reasoning behind automated decisions that may affect them, especially when these have significant legal or economic implications.

Sustainability and reduction of environmental impact

Measures will be adopted to minimise the ecological footprint associated with the development, training and implementation of AI systems, promoting the efficient use of technological resources and good environmental practices.

Traceability

All use cases must guarantee the traceability of the data used, decisions made, models employed, and processes implemented, so that they can be subject to internal or external audits, regulatory reviews, or forensic analysis if necessary.

Commitment from third parties and partners

Konecta will require third parties involved in the development, supply or implementation of AI Systems to respect the principles set out in this Policy, adopting equivalent governance, ethics and security practices.

Responsible innovation

AI will be used as a driver of innovation, creativity and continuous improvement, always in line with Konecta's ethical values and in strict compliance with current regulations, ensuring that the pursuit of efficiency or profitability does not compromise fundamental rights or the public interest.

Right to complaint and redress

Konecta recognises the right of every person to request information, file complaints or demand redress when they consider that an AI system has violated their rights. To this end, accessible, effective and transparent complaint management mechanisms will be put in place, in line with the principles of accountability and access to justice.

These principles of action respond to the impacts, risks and opportunities (IROs) arising from the applicable material issues: diversity, equality and inclusion, climate change adaptation and mitigation, information security, compliance and corporate ethics, supplier management, communication and transparency with stakeholders.

04

Prohibited practices

In compliance with the Regulation, as well as the ethical and responsibility principles assumed by Konecta, the use, development, deployment or acquisition of AI systems that engage in practices classified as inadmissible or prohibited by this Regulation is expressly prohibited by all Konecta companies.

In particular, the following uses are prohibited:

- Use of subliminal or manipulative techniques which, through stimuli below the threshold of consciousness or undetectable mechanisms of influence, alter the behaviour of individuals in such a way as to cause them significant physical or psychological harm or induce them to take decisions contrary to their interests.
- Social scoring systems, i.e., those that evaluate, classify or rate individuals on the basis of their behaviour, personal status or social characteristics, in such a way that unjustified or disproportionate adverse consequences may arise for their access to services, opportunities or rights.
- Emotional inference systems in work or educational environments, unless there is express legal justification, such as for physical security purposes or authorised medical diagnoses. This prohibition includes technologies designed to deduce the emotional state, mood or intentions of individuals based on their facial expressions, voice or physiological signals.
- Real-time remote biometric identification systems in public spaces for surveillance purposes, unless they have express legal authorisation issued by a competent authority and comply with the exceptional conditions set out in the Regulation.
- Biometric classification of individuals for the purpose of inferring sensitive characteristics, such as their ethnic origin, sexual orientation, religious or ideological beliefs, trade union membership or health status, where such inference is not legally justified and authorised in accordance with the safeguards provided for in the applicable legislation.

These practices are considered incompatible with the fundamental principles of respect for human rights, non-discrimination, individual autonomy, privacy and dignity. Konecta will use the guidelines, technical reports and guidance issued by the European Commission, the AI Office and other competent authorities as a reference for interpreting the scope and practical application of these prohibitions.

In case of doubt, no Konecta entity may implement an AI system that, directly or indirectly, could engage in the practices described above without first obtaining prior validation of its legality from the responsible internal teams or the relevant regulatory authorities and without completing the validation process established in the Responsible AI Management and Implementation Procedure.

05

AI Literacy

Suppliers and those responsible for deploying AI systems shall take measures to ensure that their staff, as well as any person using or managing such systems on their behalf, have a sufficient level of AI literacy, adapted to their roles, training, experience and the intended context of use.

The aim of AI literacy is to provide all stakeholders with the knowledge necessary to make informed decisions about the development, use and impact of AI systems.

In compliance with these provisions and in line with the principles and objectives defined in this Policy, Konecta companies will develop a set of strategic actions aimed at ensuring the responsible, safe and ethical use of AI in all their entities. These measures will be aligned with current legislation and international best practices, including the repository of good practices in AI literacy promoted by the European Commission[3].

Both employees and any third parties who suspect the existence of any potential breach related to this Policy may submit their information, questions or concerns on this matter, confidentially and without fear of reprisals, through the Information Channels available on Konecta's corporate website (https://Konecta.integrityline.com), depending on the nature of the situation, in accordance with procedure PG COR 26 Information Channels, available on the same website, which specifies the different channels available and the nature of the communication that can be made through them.

This channel is available 24 hours a day, 7 days a week. No reprisals will be tolerated against anyone who, in good faith, reports facts that could constitute a breach of this policy, and the guarantees and protections established by the applicable regulations and legislation will apply to those who report.

Breaches of this policy will be subject to the corresponding disciplinary measures in accordance with internal rules and procedures, without prejudice to any administrative or criminal penalties that may also result from such breaches and which may be imposed by the competent authority.

[3] Available on https://digital-strategy.ec.europa.eu/es/library/living-repository-foster-learning-and-exchange-ai-literacy

06

Policy governance

Policy Ownership

The responsibility for drafting, maintaining and updating this Policy lies with the Legal Department responsible for the Governance framework. However, its initial approval and any subsequent amendments shall be the responsibility of the Board of Directors.

Interpretation

The Board of Directors shall be responsible for the official interpretation of this Policy. In the event of any discrepancy between different language versions, the Spanish version shall always prevail as the authentic and binding version for all purposes.

07

Updating and revision

The Artificial Intelligence Management and Governance Policy will be reviewed periodically or when necessary to adjust it to changes in the business model, the approval of new regulations or international best practices, ensuring its effectiveness and ongoing compliance.

NOTE: This Policy has been approved on December 16, 2025, by the highest governing body and replaces any previous version of it, with only this document being valid from this date onwards.

Version Control

Version	Review date	Reviewed	Validated	Approved	Reason for change
1	12/16/2025	IT_Information Security Organization & Procedure	Legal Affairs	Board of Directors	Initial edit