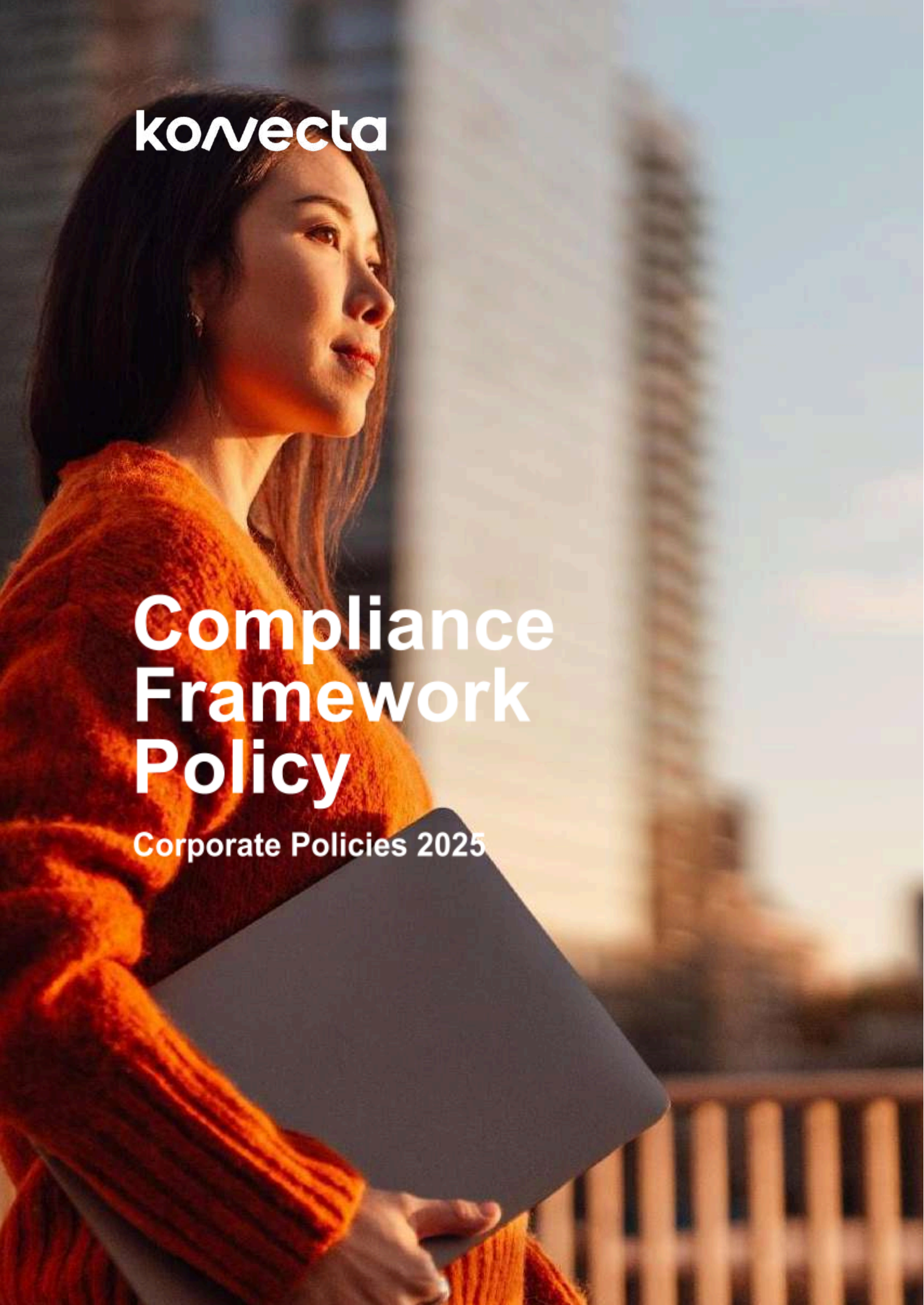


# Compliance Framework Policy

## Corporate Policies 2025

# Table of contents

# 01 Purpose

The objective of this Compliance Framework Policy (hereinafter, the “Policy”) is to establish and disseminate the basic and general rules of Konecta, a multinational group of companies specialising in the provision of digital customer management services and solutions (hereinafter, Konecta, the Company or the Firm), in terms of compliance with applicable regulations, including criminal law, which allows for the development of honest, ethical and transparent professional conduct in line with human rights, as well as showing firm rejection of any kind of irregularity, without, in any case, its commission being justified on the basis of a benefit for the organisation.

In this regard, Konecta's Management Body has worked on the implementation of a Compliance and Criminal Risk Prevention Model (hereinafter, the “Compliance Model” or the “Model”), thereby reinforcing and promoting an ethical business culture that establishes appropriate control and management mechanisms in the area of detecting and preventing regulatory risks and non-compliance, whether directly or indirectly, expressly stating its rejection of any illegal or unethical act.

Konecta's corporate governance system is inspired by and based on a commitment to ethical principles, integrity and leadership in the application of best practices, structured around the defence of social interests and the creation of sustainable value for the company, its employees, suppliers and customers. As such, this Policy is an extension of Konecta's regulatory framework and responds to the expectations of its stakeholders (employees, customers, partners and shareholders, investors, financial institutions, suppliers, public administration and regulatory bodies), ensuring scrupulous compliance with the laws and regulations in force in each country, its own requirements and international standards.

This Policy develops the provisions of the Code of Ethics, as well as the company's existing internal policies, manuals and procedures on the subject.

02

# Scope of application

This Policy applies globally to all Konecta entities as part of its Compliance Programme and is endorsed by the company's senior management.

Every member of the company is responsible for promoting the principles and commitments set out herein in their workplace. Consequently, it must be observed by all Konecta employees, regardless of their position or role within the organisation or their geographical location, in relation to the activity they carry out and which has been deemed to expose them to certain criminal risks.

Notwithstanding the foregoing, Konecta will encourage the application of this Policy to all individuals and/or legal entities linked to the company by a relationship other than employment: suppliers, contractors and workers in the supply chain, and business partners, in compliance with the Law and as a demonstration of due diligence.

Given that many of Konecta's companies have their registered office outside the European Union, internal regulations will be adapted to the regulations of each State where necessary, respecting and ensuring compliance with the basic principles set out herein.

In addition to this Policy, there is a criminal risk matrix that lists the behaviours classified in Article 31 bis of the Spanish Criminal Code, according to which companies could be investigated in Spain for crimes committed in the name or on behalf of the companies and for their direct or indirect benefit, (i) by their legal representatives and de facto or de jure administrators, or (ii) by persons subject to their authority, when the commission of the offence, in the latter case, is the result of a lack of proper control, taking into account the specific circumstances of the case.

03

# General principles of action

Konecta has embraced the desire to promote a culture of ethics and compliance, respect for applicable regulations and voluntarily assumed commitments, as well as adaptation to best practices in compliance that enable the development of diligent professional conduct, demonstrating the company's firm condemnation of any kind of illegal, criminal or other act, which cannot be justified on the basis of a benefit to the organisation.

Konecta's Compliance Model includes the organisation's criteria for action and control elements that prevent non-compliance with obligations and commitments within its sphere of activity. Without prejudice to the provisions of the Code of Ethics, Konecta's Compliance and Criminal Risk Prevention Model is based on the following general principles, which constitute the fundamental basis of both the company's internal regulations and the conduct of its employees:

Foster a culture of prevention based on the principle of “zero tolerance” towards the commission of irregularities in any regulatory area, promoting the application of the principles of ethics and responsible behaviour by all professionals acting on behalf and/or representing Konecta.

- Absolute rejection of any act that could be considered a crime: Konecta is firmly committed to ensuring compliance with current criminal law and does not accept any type of infringement in relation to it.
- Absolute rejection of any type of conduct that could be construed as corrupt: both in relations with civil servants and public administrations, and with other third parties with whom business relations are maintained.

Compliance with the law and internal regulations: Konecta, and in particular its Management Body and its directors, shall act and require all employees to act at all times in accordance with the provisions of current legislation and the Criminal Risk Prevention and Compliance Model.

- Compliance with accounting obligations and financial reporting: Konecta's financial reporting shall be prepared with reliability and rigour, complying with all internal control procedures established to ensure the correct accounting of transactions and their accurate reflection in Konecta's financial reporting.
- Respect for intellectual and industrial property: Konecta employees shall respect the intellectual property and right of use belonging to the company in relation to courses, projects, computer programmes and systems, knowledge, processes, technology, know-how and, in general, other works and projects developed or created by Konecta or any third party.
- Protection of personal data: Konecta employees shall protect the personal data of both employees and any other persons whose data may be accessed as a result of Konecta's activities, in accordance with applicable regulations and in compliance with the company's internal processes.
- Secrecy and confidentiality: Konecta employees shall maintain professional secrecy with regard to any non-public data or information they become aware of as a result of their professional activity, whether it originates from or refers to customers, suppliers, Konecta, employees, managers or any third party.

- Equal opportunities and non-discrimination: in access, promotion, training, remuneration and other working conditions, with the principle of objectivity taking precedence in all actions and decisions.

**Relationships with third parties:**

- Provide a regulatory and compliance framework with those third parties with whom we may have business relationships, in order to ensure integrity and honest practices within the framework of free competition.
- Ensure Konecta's commitment to its customers through the creation of quality services that contribute to meeting customer requirements and expectations.

  Within this framework, the Group absolutely rejects any type of advertising, commercial or promotional activity that misleads or may mislead its customers, committing to providing clear information about its services.
- Promote self-control processes in the actions and decision-making of Konecta members, so that they take into account four basic premises:

  (I) that the action complies with the Code of Ethics;
  (II) that it is legally valid;
  (III) that it is aligned with the company's strategic objectives;

  (IV) that it falls within the scope of their competences and that, therefore, they must assume responsibility for it.
- Develop specific procedures for the prevention, detection and management of non-compliance, such as internal audits, periodic controls or risk assessments, in order to anticipate possible infringements and respond in a structured and effective manner.
- Prevention of criminal risks: the company is committed to risk prevention, including those of a criminal nature. To this end, and in accordance with Spanish legislation, Konecta has implemented a Criminal Risk Prevention Model.
- Strengthen the authority and independence of the Compliance Committee as the body responsible for ensuring the proper functioning of the Compliance Model, as well as other applicable internal regulations.
- Disseminate among the members of the organisation the rules, policies and procedures that should govern their actions within the Group and the necessary tools for this purpose.
- Raise awareness, train and sensitise (as appropriate in each case) both the members of the organisation and the value chain of the importance of acting in accordance with current legislation and complying with the commitments voluntarily assumed by Konecta in the performance of its duties.
- Make the appropriate information channels available to all members of the organisation, establishing the duty to report and denounce in good faith any irregular conduct of which they are aware or suspect. Konecta guarantees, in all cases, the confidentiality of those reported and those reporting, as well as the absence of reprisals against those reporting in good faith.

- Environmental protection: Konecta is actively and responsibly committed to environmental conservation, complying with legal requirements and striving to reduce the environmental impact of its activities.
- Occupational risk prevention: Konecta is aware of the importance of the health and safety of its workers, establishing the achievement of physical, mental and social well-being as a fundamental pillar within the company's preventive culture.

These principles of action respond to the impacts, risks and opportunities (IROs) arising from material issues related to corporate governance.

**Basis of the Model**

Konecta's Criminal Risk Prevention and Compliance Model (hereinafter, the Model) is a compilation of the procedures and controls in place within the Group that prevent, detect or enable a response to the commission of possible illegal acts and is part of Konecta's Compliance Programme. It essentially comprises the following elements:

- Compliance Committee: is the body responsible for ensuring the proper functioning of the Model, with the independence and authority necessary to perform its duties.
- Compliance Function Statute: establishes the basis for the Compliance Function, its bodies and those responsible for it, as well as its interrelationship with other areas and stakeholders, defining its principles of action and internal regime.
- Compliance Framework Policy: highlight's the Group's rejection of any unlawful behaviour and its commitment to ethics and compliance and its members to act with integrity.
- Code of Ethics: Konecta has a Code of Ethics accessible to all its employees, which sets out the values, principles and guidelines of conduct that must govern the professional behaviour of the Group.
- Code of Ethics for Suppliers: its purpose is to establish the minimum standards and commitment that the company's suppliers must maintain with regard to the basic principles of ethics, honesty and professionalism.
- Criminal risk map: this forms the basis for identifying the criminal risks to which Konecta is exposed due to its activities.
- Information channels: Konecta has a communication channel that allows employees to report any potentially significant irregularities that, in their opinion, constitute a violation of the principles set out in the Compliance and Criminal Risk Prevention Model.
- Supervision and monitoring system: the supervision and monitoring system allows for continuous validation of the implementation of the Model, periodically checking the effectiveness of existing policies, procedures and controls, as well as their evolution, so that the company has an overview of the activity carried out in this area, enabling it to take the necessary actions to

ensure its adequacy and effectiveness in the performance of its risk prevention, management and control functions.

- Economic and financial management model: Konecta has a series of controls and procedures in place in the financial and economic sphere that ensure full transparency and accuracy in its accounting records, transactions and, in general, the Group's economic management.

- Disciplinary system: all Konecta employees are required to comply with the Code of Ethics and the company's policies and procedures; therefore, any conduct contrary to this obligation will result in disciplinary measures being applied in accordance with Konecta's internal regulations, which in no case will be contrary to applicable labour regulations.

**Roles and responsibilities**

- All employees to whom this Policy applies must comply with it and take the necessary actions to follow it, in accordance with their duties and responsibilities, as well as attend any training sessions they are required to attend related to it and the principles of action it advocates.

- Board of Directors and Board Committees: approval or modification of Konecta's general policies and strategies.

- This Policy reinforces the commitment of Konecta's Board of Directors and Senior Management to defending compliance with the law, as well as communicating and disseminating the principles contained in the Compliance and Criminal Risk Prevention Model.

- Due to its proximity to strategic and operational objectives and its hierarchical position, Senior Management is responsible for directing and supporting all members of the Group in the exercise of their compliance obligations, ensuring the availability of adequate and sufficient resources for the effective implementation of measures.

    - Participates in the analysis and assessment of criminal risks when required to do so.

- Compliance Committee:
    - It is the body responsible for ensuring the proper functioning of the Model, with the independence and authority necessary to perform its duties.
    - Review the criminal risk matrix.
    - Ensure the diligent processing of communications regarding breaches of the Compliance Model, guaranteeing the confidentiality of information at all times.

- Compliance Department:
    - Ensure the effective implementation of this Policy through appropriate measures, including the development of a monitoring system.

- Promote training and awareness of this Policy.
- Support the different areas of the company in the implementation of this Policy.

**Communication and training**

This Policy will be available on the corporate website (www.Konecta.com).

**Prevention and responsibility**

Both employees and any third party 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), 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 retaliation 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 the reporting parties.

Breaches of the Code of Ethics 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.

04

# Updating and revision

The Compliance Framework Policy will be reviewed and updated periodically, or whenever necessary to adjust it to changes in the business model, or that may occur within Konecta's field of activity, or as a result of the approval of directly applicable regulations, ensuring its effectiveness and continued compliance.

NOTE: This Policy has been reviewed and 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 | 12/19/2022 | Compliance<br>Organization & Procedure | Legal Affairs | Board of Directors | Initial edit |
| 2 | 12/16/2025 | Compliance<br>Organization & Procedure | Legal Affairs | Board of Directors | Alignment with legal requirements<br>Alignment with the new format and branding<br>Consolidation of the framework policy and its dependent policies into a single document |

# Annex 1. Policy on the prevention of corruption, bribery and money laundering

Corporate Policies 2025

# Table of contents

# Purpose

## Annex 1

The purpose of this Policy for the Prevention of Corruption, Bribery, and Money Laundering (hereinafter, the “Policy”), which forms part of the Compliance Framework Policy, is to establish and disseminate the basic and general rules of Konecta, a multinational group of companies specialising in the provision of digital customer management services and solutions, (hereinafter, Konecta, the Company, or the Firm) to prevent corrupt business practices and money laundering, in order to contribute to business transparency and improve the company’s competitiveness in favour of fair competition.

As a signatory to the United Nations Global Compact, which the company joined in 2004, Konecta is committed to Principle No. 10, which advocates the fight against corruption in all its forms. Likewise, in order to contribute to the agenda set by the United Nations for sustainable development, Konecta has adopted the Sustainable Development Goals within the framework of the 2030 Agenda.

# Scope of application

## Annex 1

This Policy falls within the scope of the Compliance Framework Policy and applies to all Konecta entities, backed by the company's senior management.

Consequently, its content must be observed by all Konecta employees, regardless of their position or role within the organisation or their geographical location.

Notwithstanding the foregoing, its scope of application may be extended, when necessary and possible due to the nature of the relationship, to all individuals and/or legal entities linked to Konecta on a business or professional basis, through a relationship other than employment: suppliers, contractors and workers in the supply chain, and business partners.

Given that many of Konecta's companies have their registered office outside the European Union, the internal regulations will be adapted to the regulations of each State where necessary, respecting and ensuring the basic principles set out herein.

# General principles of action

## Annex 1

Konecta maintains a zero-tolerance policy towards any type of corruption, bribery, fraud, embezzlement, and other undue benefits, whether involving public officials or private individuals. This principle is absolute and prevails over any potential benefit to the company or its stakeholders if it derives from a transaction that is irregular, illegal, or contrary to the law or the Code of Ethics.

Aware that each of the countries in which the Group operates has a different social context and different needs, this Policy for the Prevention of Corruption, Bribery and Money Laundering is articulated through plans and actions related to the principles set forth herein, adapted to the reality of each of its local operations, taking into account the social appropriateness of the conduct and in accordance with the laws of the country.

There are certain principles, which, without being *numerus clausus*, constitute an important starting point that Konecta has adopted to ensure that, through its business activities, corruption is adequately prevented, thus contributing directly to transparency and respect for fair competition, generating value:

- Compliance with the principles of good corporate governance.
- Implementation of a Code of Ethics within the company.
- Implementation of a regulatory compliance program.
- Implementation of information channels -whistleblowing channel- to report possible breaches of the company's internal rules and/or legal regulations.
- Public information on contracts with the public sector and information on activities subsidised with public aid.
- Public information on corporate policies.
- Avoidance of favoritism and corruption in the private sector.
- Avoidance of corruption practices by foreign officials in international transactions.
- Compliance with tax obligations.

## Prohibited corrupt practices

### Corruption of public officials and private individuals

It is prohibited to give, promise, or offer any kind of payment, commission, gift, or reward to any authorities, public officials, or employees or managers of public companies or organisations, whether directly to them or indirectly through persons or companies linked to or acting on their behalf, whether the recipient is the public official or employee themselves or another person designated by them.

This prohibition extends to any employees, executives, or administrators of other companies or entities, whether directly or indirectly, with the aim of favouring Konecta over its competitors by breaching their obligations in the contracting of products, services, or the sale of goods.

Such deliveries, promises, or offers are prohibited whether they are made directly by a Konecta company or indirectly through partners, collaborators, agents, intermediaries, brokers, advisors, or any other intermediaries.

Unless, due to their frequency, characteristics, or circumstances, they could be interpreted by an objective observer as being intended to influence the impartial judgement of the recipient, the following situations are not included in this prohibition, provided that they comply with the established guidelines on this matter:

- Advertising items of little value.
- Normal invitations that do not exceed the limits considered reasonable in customary, social, and courtesy practices.
- Occasional gifts for specific and exceptional reasons (such as Christmas gifts), provided that they are not in cash and are within modest and reasonable limits.
- Invitations to sporting or cultural events sponsored by Konecta.

Persons subject to the Code must reject and report to the Compliance Committee any request by a third party for payments, commissions, gifts, or remuneration of the type mentioned in the first paragraph.

**Agents, intermediaries, and advisors**

The use of agents, intermediaries, or advisors in transactions or contracts in which a public administration, public body, or public company is involved in any way shall require the adoption of the following measures:

- Whenever possible, entities of recognised prestige in the market or sector in question shall be used as agents, intermediaries, or advisors, and, if feasible, leading companies, especially when the remuneration of the agent, intermediary or advisor is linked to the success of the transaction or contract.
- Due diligence mechanisms shall be implemented to try to get to know, as far as is reasonable, the persons involved and their collaborators, so that the most suitable ones can be chosen, reasonably ensuring that they are trustworthy and do not, as a result, carry out activities that may involve risks, economic damage or compromise the reputation and good image of Konecta.

### 3.2. Prevention of money laundering

This is Konecta's approach: to ensure the effectiveness of the security measures implemented, guided by the following principles:

- Company management must be aware of the risks of money laundering and terrorist financing and ensure that the necessary measures are taken to effectively mitigate these risks.
- Communication between the different departments of Konecta must be constant in order to detect any behaviour that may pose a risk, with the aim of establishing the necessary measures to mitigate it.
- Prevention protocols must be established in accordance with the principle of universality.

- The procedures implemented will be fully adapted to Konecta's business, seeking to know the origin of the funds and the consistency of the transaction carried out, and will be reviewed periodically.

Specifically, employees must ensure that, in the course of their activities, they comply with policies and procedures aimed at preventing and controlling money laundering and terrorist financing, taking into account the following:

- Ensure that customers linked to the company meet quality and character requirements such as there is always recognised moral integrity and lawful and transparent activity. The financial capacity of customers must be consistent with their activity and with the transactions or operations they carry out at the entity.
- When information about the suspicious activity of a customer or supplier becomes known and it is considered that the business relationship between them and the company should not be extended, immediate notice must be given to superiors in order to unify criteria, prevent unfavourable repercussions, and send the relevant reports to the competent authority.
- Ensure compliance with regulations to prevent and control conduct related to this phenomenon, avoiding risks in the company's operations.

Employees must always prioritise ethical principles over commercial goals.

### Controls

- Ethical business relationships: the company prioritises business relationships with partners and entities that demonstrate integrity, good reputation, and a strong commitment to social, environmental, and governance criteria.
- Accurate accounting records: the company's operations, transactions, and actions must be accurately and appropriately reflected in the accounting books and records.
- Conflicts of interest: Special attention will be paid to situations that may give rise to conflicts of interest between staff, partners, and the company.
- Tax obligations: Illegal tax evasion practices and the use of opaque structures for tax purposes will be avoided.

### Training and collaboration:

- Training: Training and awareness programs will be offered with a special emphasis on those roles most exposed, to ensure knowledge and application of this Policy.
- Active collaboration: the company will cooperate in good faith with internal and external audits related to this matter.

These principles of action respond to the impacts, risks and opportunities (IROs) arising from the applicable material issues: compliance and corporate ethics, supplier management, communication and transparency with stakeholders.

Both employees and any third party who suspects the existence of any potential breach related to this Policy or the Code of Ethics may submit their information, questions, or concerns on this matter confidentially and without fear of reprisals through the Information Channels available on the corporate website at the following URL: https://Konecta.integrityline.com, depending on the nature of the situation, in

accordance with procedure PG COR 26 Information Channels, available in the same space, 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 retaliation 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 applicable regulations and legislation will apply to whistleblowers.

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 and be imposed by the competent authority.

# Updating and revision

## Annex 1

The Policy on Prevention of Corruption, Bribery, and Money Laundering 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 continued compliance.

NOTE: This Policy was reviewed and approved on December 16, 2025, by the highest governing body and replaces its previous version, with only this document being valid from the date of approval.

**Version Control**

| Version | Review date | Reviewed | Validated | Approved | Reason for change |
|---|---|---|---|---|---|
| 2 | 22/06/2021 | Compliance<br>Organization & Procedure | Legal Affairs | Board of Directors | General Policy Review |
| 3 | 19/12/2022 | Compliance<br>Organization & Procedure | Legal Affairs | Board of Directors | General Policy Review |
| 4 | 12/16/2025 | Compliance<br>Organization & Procedure | Legal Affairs | Board of Directors | Alignment with legal requirements<br>Alignment with the new format and branding |

# Annex 2. Privacy and confidentiality policy

Corporate Policies 2025

# Table of contents

# Purpose

## Annex 2

The objective of this Privacy and Confidentiality Policy (hereinafter, the “Policy”), which forms part of the Compliance Framework Policy, is to establish and disseminate the basic and general rules of Konecta, a multinational group of companies specialising in the provision of digital customer management services and solutions (hereinafter, Konecta, the Company or the Firm), related to the preventive and proactive responsibility of the principle of security and accountability, to guarantee privacy and the fundamental right to the protection of personal data for which Konecta is responsible, as well as those it accesses in its capacity as data processor during the provision of services to its customers, ensuring, in all cases, scrupulous compliance with applicable legislation.

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 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.

# Scope of application

## Annex 2

Consequently, its content is mandatory for all Konecta employees, regardless of their position or role within the organisation or their geographical location.

Notwithstanding the foregoing, its scope of application may be extended, when necessary and possible due to the nature of the relationship, to all individuals and/or legal entities linked to Konecta on a business or professional basis, through a relationship other than employment: suppliers, contractors and workers in the supply chain, and business partners.

Given that many of Konecta's companies have their registered office outside the European Union, internal regulations will be adapted to the regulations of each State where necessary, respecting and ensuring compliance with the basic principles set out herein.

# General principles of action

## Annex 2

Konecta values and respects both its own and its clients' trade secrets, as well as industrial and intellectual property rights. For this reason, confidentiality is a tool for managing its business competitiveness and encompasses the protection of information ranging from business data relating to clients and suppliers to commercial plans and market studies or strategies, among others.

Aware that each of the countries in which the company operates has a different social context and different needs, this Privacy and Confidentiality Policy is articulated through plans and actions related to the principles set out therein, adapted to the reality of each of its local operations.

Based on Konecta's utmost respect for the applicable legislation on personal data protection, the general principles of action in relation to data processing are as follows:

- Lawfulness, fairness and transparency: personal data will be processed lawfully, fairly and transparently, so that the data subject is aware of how their data will be processed, if applicable.
- Purpose limitation: personal data shall be collected for specific, explicit and legitimate purposes and shall not be further processed in a manner incompatible with those purposes.
- Data minimisation: personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are used.
- Accuracy: personal data shall be accurate and, where necessary, kept up to date. Every reasonable measure shall be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Storage limitation: personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Integrity and confidentiality: personal data shall be processed in such a manner as to ensure appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. All this shall be in accordance with applicable legislation and the provisions of mandatory internal regulations on information security.
- Information: the processing of personal data shall be transparent in relation to the data subject, providing them with information about the processing of their data in an understandable and accessible form, when required by applicable law. In order to ensure fair and transparent processing, the Company shall inform the data subjects or interested parties whose data is to be collected of the circumstances relating to the processing in accordance with the applicable regulations.
- Accountability: Konecta shall be responsible for complying with the principles set out in this Policy and in the applicable regulations on personal data protection and privacy, and shall be able to demonstrate this when required by these regulations.
- International data transfers: any processing of personal data subject to European Union regulations that involves a transfer of data outside the European Economic Area must be carried out in strict compliance with the requirements established in the applicable law in the jurisdiction of origin.

- Risk-based approach: when an activity involves the processing of personal data that may pose a high risk to the rights and freedoms of the data subject, to the extent and in the manner required by the regulations, Konecta will carry out a risk and impact assessment on the protection of personal data and privacy before the processing begins.
- Rights of data subjects: the company will allow data subjects to exercise their rights of access, rectification, erasure, restriction of processing, portability and objection as applicable in each jurisdiction, establishing, for this purpose, the internal procedures necessary to satisfy, at least, the legal requirements applicable in each case.

Konecta will always inform data subjects in clear and simple language about how their data is processed, emphasising that all personal data is kept confidential and with adequate security, taking into account the characteristics of the data.

Of particular relevance is the role that Konecta adopts when providing services to its clients: data processor.

These principles of action respond to the impacts, risks and opportunities (IROs) arising from the applicable material issues: compliance and corporate ethics, supplier management, communication and transparency with stakeholders.

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.

Failure to comply with 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 this and which may be imposed by the competent authority.

# Updating and revision

## Annex 2

The Privacy and Confidentiality Policy will be reviewed periodically or when necessary to bring it into line with 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 |
|---|---|---|---|---|---|
| 2 | 06/22/2021 | Compliance<br>Organization & Procedure | Legal Affairs | Board of Directors | General Policy Review |
| 3 | 12/19/2022 | Compliance<br>Organization & Procedure | Legal Affairs | Board of Directors | General Policy Review |
| 4 | 12/16/2025 | Compliance<br>Organization & Procedure | Legal Affairs | Board of Directors | Alignment with legal requirements<br>Alignment with the new format and branding |

# Annex 3. Information systems security and cybersecurity policy

Corporate Policies 2025

# Table of contents

# Purpose

## Annex 3

The objective of this Information Systems Security and Cybersecurity Policy (hereinafter, the “Policy”), is to establish and disseminate the basic and general rules of Konecta, a multinational group of companies specialising in the provision of digital customer management services and solutions (hereinafter, Konecta, the Company or the Firm), to guarantee the integrity, privacy and confidentiality of information, in accordance with current legislation on the matter, weighing up the risks and making efficient use of resources, all based on criteria of proportionality in management.

The widespread use of information and communication technologies (ICT) in all areas of society has created a new space, cyberspace, where conflicts and attacks can occur, and cyber threats exist that could harm Konecta and its various companies.

This Policy establishes a framework that sets out the principles for ensuring the protection of Konecta's information systems against unauthorised access, loss or damage during information processing or other types of cyber threats, guaranteeing the availability, integrity and confidentiality of the information in the data managed by Konecta.

This Policy is designed to establish the framework for Konecta's internal stakeholders (employees, shareholders, investors, executives) and external stakeholders (customers, suppliers, auditors, governments, regulatory bodies, the media, competitors and financial institutions), enhancing confidence in the company's information systems and ensuring scrupulous compliance with current regulations in each country, internal requirements and international standards.

This Policy will be available on the corporate website (Konecta.com) to ensure that it can be consulted by all interested parties.

# Scope of application

## Annex 3

This Policy falls within the scope of the Compliance Framework Policy and extends to all Konecta entities, backed by the company's senior management.

Consequently, its content is mandatory for all Konecta employees, regardless of their position or role within the organisation or their geographical location.

Notwithstanding the foregoing, its scope of application may be extended, when necessary and possible due to the nature of the relationship, to all individuals and/or legal entities linked to Konecta on a business or professional basis, through a relationship other than employment: suppliers, contractors and workers in the supply chain, and business partners.

Given that many of Konecta's companies have their registered office outside the European Union, internal regulations will be adapted to the regulations of each State where necessary, respecting and ensuring compliance with the basic principles set out herein.

# General principles of action

## Annex 3

The Information Systems Security and Cybersecurity Policy reflects the Company's express commitment to determining and establishing guidelines and adequate support for the administration of the security of the information it handles, in accordance with its own requirements and with current laws and regulations.

Konecta strives to ensure “the secure use of networks and information systems by strengthening our capabilities for prevention, defence, detection, analysis, investigation, recovery and response to cyberattacks” that may occur.

Konecta advocates promoting the secure use of information systems and telecommunications, always in line with the business strategy and objectives. In this regard, it has set the following specific objectives, which are consistent with the context in which the company's activities are carried out:

- Promoting the security and resilience of the networks and information systems used.
- Raising awareness among all company personnel of the risks arising from cyberspace.
- Training and maintaining the knowledge, skills, experience and technological capabilities to support Konecta's cybersecurity objectives.

In this regard, Konecta undertakes to achieve the following objectives:

- Consider information and the systems that support it as strategic assets. Konecta therefore expresses its determination to achieve the necessary security levels to guarantee the confidentiality, integrity and availability of the information processed within the organisation and of the information system resources that process, store or distribute it.

- Ensure the dissemination of the regulations defined in support of this Policy, with the aim of instilling in Konecta's staff a level of awareness and training in information security that guarantees the application of appropriate practices in this area, as an inherent part of the performance of their duties.

- Promote the achievement of the required levels of information security as a continuous process of improvement and constant progress, based on the definition of the objectives and requirements to be met, the implementation of the appropriate processes and measures, the verification of their effectiveness, efficiency and efficacy, and the adoption of the appropriate corrections and modifications.

- This Policy should be the main tool for adequately guaranteeing Information Security, promoting and ensuring compliance within the different services.

- Ensure the existence of the necessary mechanisms to guarantee the continuity of the company's critical activities that are supported by information systems, allowing for their recovery within an acceptable period of time.

- Maximise the quality of services provided.

- Reduce or eliminate, as far as possible, the dangers and risks in the assets, processes and services provided by Konecta.
- Determine essential information security measures that Konecta must adopt to protect itself appropriately against threats that could affect the confidentiality, integrity and availability of information in any way.

The objectives of this Policy will be implemented based on a long-term strategy. Activities to achieve the objectives must be maintained over time.

In line with security risks, action plans must be defined and adjusted each year (security controls, definition of security projects, continuous monitoring, etc.).

The necessary transition plans will be established to reduce any impact on Konecta's activities and/or resources, and Konecta will also ensure that employees:

- … are familiar with and apply Konecta's internal procedures and protocols regarding information security.
- … have tools that allow them to easily access internal operating procedures (Intranet). In addition, alternative communication channels will be used to communicate certain processes, special measures or procedural updates.
- … are aware that they must only process the information for which they have been authorised and use Konecta's assets solely for the performance of their professional duties. Employees must comply with the basic rules for accessing applications and/or equipment with access to personal data.
- … are familiar with the company's existing procedures so that they know how to act in the event of any activity or threat that may affect information security, and must inform the Technology Department and the Chief Information Security Officer (CISO).

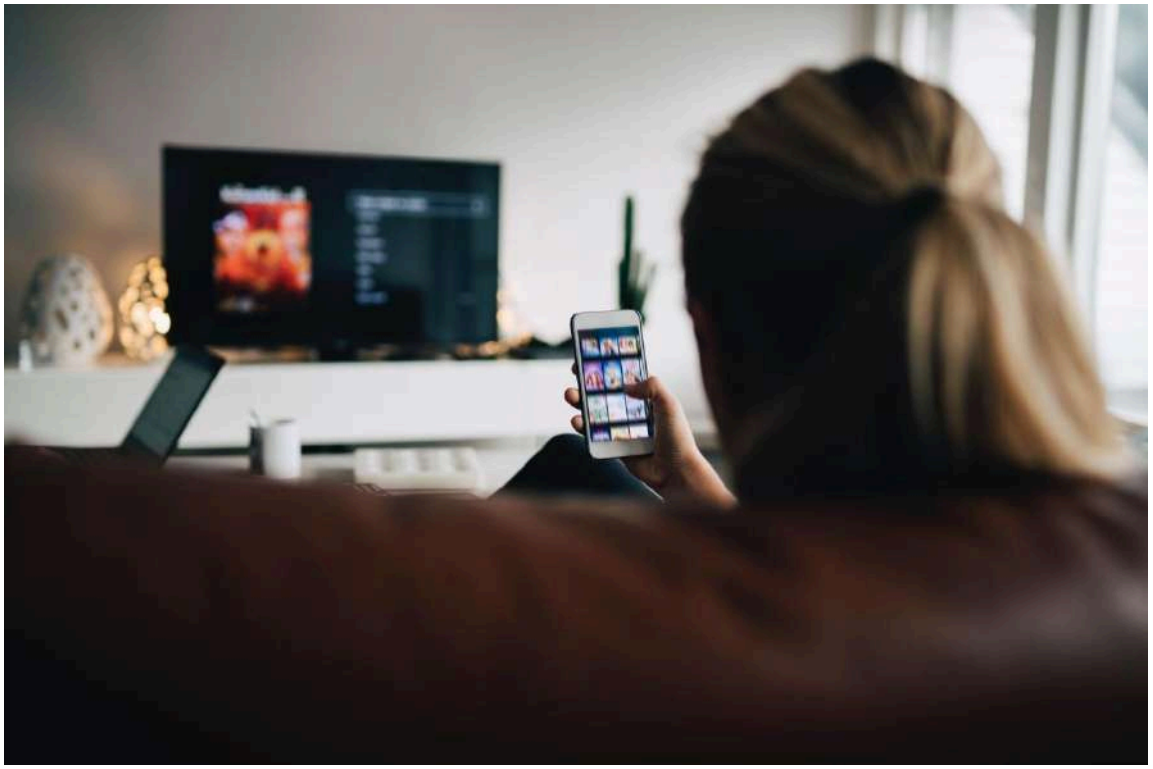
Aware that each of the countries in which the company operates has a different social context and different needs, this Privacy and Confidentiality Policy is articulated through plans and actions related to the principles set out therein, adapted to the reality of each of its local operations.

These principles of action respond to the impacts, risks and opportunities (IROs) arising from the applicable material issues: information security, digital transformation, compliance and corporate ethics, and suppliers' management.

Both employees and any third parties who suspect the existence of any potential breach related to this Policy or to the Code of Ethics, 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.

Failure to comply with 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 this and which may be imposed by the competent authority.



# Updating and revision

## Annex 3

This Policy lays the foundations for compliance with the following standards:

- ISO/IEC 27001:2022 Information technology -Security Techniques-Information security management systems - Requirements.
- ISO/IEC 27701- Extension of ISO 27001 for privacy management.
- ISO/IEC 27002:2022 Information technology - Security techniques - Code of practice for information security controls.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).
- Personal Data Protection Laws applicable in each country.

The Information Systems Security and Cybersecurity Policy will be reviewed periodically or when necessary to bring it into line with 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 |
|---|---|---|---|---|---|
| 2 | 06/22/2021 | IT_Information Security<br>Organization & Procedure | Legal Affairs | Board of Directors | General Policy Review |
| 3 | 12/19/2022 | IT_Information Security<br>Organization & Procedure | Legal Affairs | Board of Directors | General Policy Review |
| 4 | 12/16/2025 | IT_Information Security<br>Organization & Procedure | Legal Affairs | Board of Directors | Alignment with legal requirements<br>Alignment with the new format and branding |

# Annex 4. Artificial intelligence management and governance policy

Corporate Policies 2025

# Table of contents

# Introduction

## Annex 4

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.

# Scope of application

## Annex 4

This corporate policy falls within the scope of the Compliance Framework Policy and shall apply to all companies that form part of Konecta Group. 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.

# Guiding principles applicable to use cases

## Annex 4

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.

# Prohibited practices

## Annex 4

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.

# AI Literacy

## Annex 4

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

# Policy governance

## Annex 4

## 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.

# Updating and revision

## Annex 4

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<br>Organization & Procedure<br>GenAI | Legal Affairs | Board of Directors | Initial edit |

konvecta

# Annex 5. Fiscal policy

Corporate Policies 2025

# Table of contents

# Purpose

## Annex 5

The objective of this Fiscal Policy (hereinafter, the “Policy”), which forms part of the Compliance Framework Policy, is to lay the foundations for the development and effective implementation of the guiding principles in tax matters of Konecta, a multinational group of companies specialising in the provision of digital customer management services and solutions (hereinafter, Konecta, the Company or the Firm).

This Policy is an extension of Konecta’s regulatory framework to respond to the expectations of its stakeholders (employees, customers, partners and shareholders, investors, financial institutions, suppliers, public administration and regulatory bodies), ensuring scrupulous compliance with the laws and regulations in force in each country, its own requirements, and international standards. This Policy will be available on the corporate website (www.Konecta.com) to ensure that it can be consulted by all interested parties.

In this regard, Konecta is committed to complying with applicable tax regulations and all tax practices carried out in accordance with good tax practices.

# Scope Of Application

## Annex 5

This Policy falls within the scope of the Compliance Framework Policy and applies to all Konecta entities, backed by the company's senior management.

Consequently, its content must be observed by all Konecta employees, regardless of their position or role within the organisation or their geographical location.

Notwithstanding the foregoing, its scope of application may be extended, when necessary and possible due to the nature of the relationship, to all those individuals and/or legal entities linked to Konecta on a business or professional basis, through a relationship other than employment: suppliers, contractors and workers in the supply chain, and business partners.

The following have more specific responsibilities related to this Policy:

## Board of Directors:

- Approval of investments or operations of any kind that are strategic in nature.

## Finance Department:

- Supervision of the application of the guiding principles of this Policy.
- Coordination and processing of information on Konecta's tax practices.
- Promoting communication between the Tax Department and the various areas involved in any tax-related process.

## Financial and Tax Department Management:

- Manage tax matters by applying good tax practices and acting transparently.
- Give priority attention to the responsible fulfilment of Konecta companies' duty to pay the taxes required in the countries where they operate.
- Reconcile responsible compliance with tax obligations with the commitment to create value for partners through efficient management of tax costs and benefits.
- Control the effective implantation of the fundamental aspects of the Tax Policy in any tax process carried out in the company, establishing the appropriate internal control procedures and measures for this purpose.
- Efficient management of tax costs and application of tax incentives and benefits permitted by applicable law.
- Orderly management of tax matters to ensure compliance with tax obligations and tax management.
- Reporting to the Board of Directors on the implementation of the tax strategy and policy.
- Maintaining a duly updated risk map that specifically identifies the tax risks arising from the tax policies applied, possible non-compliance, disputes over the application of laws or legal instability.
- Submitting the updated risk map to the General Management.

- Review and update of this Tax Policy for subsequent ratification by the General Financial Management and the Board of Directors.

Given that many of Konecta's companies have their registered office outside the European Union, internal regulations will be adapted to the regulations of each State, respecting and ensuring compliance with the basic principles set out herein.

# General principles of action

## Annex 5

## Principles of fiscal strategy

Konecta's Finance Department will ensure that tax obligations are met in accordance with good tax practices, paying the taxes that are due in accordance with the legal system.

In this regard, the Code of Ethics, which is binding on all Konecta employees, stipulates that all practices involving the illegal evasion of tax payments to the detriment of the Treasury shall be avoided, as shall the use of opaque structures for tax purposes, designed with the aim of preventing the tax authorities from identifying the person ultimately responsible for the activities or the ultimate owner of the assets or rights involved.

Relations with the tax authorities in the countries where Konecta operates are based on the principles of transparency, loyalty, collaboration, good faith and mutual trust. To this end, the company makes the greatest possible use of cooperative tax compliance mechanisms with the tax authorities of the different countries in which it operates, without prejudice to any legitimate disputes that may arise with those authorities as a result of the interpretation of the applicable rules in defence of the company's interests.

Konecta is committed to complying with applicable tax regulations and all tax practices are carried out in accordance with good tax practices.

## Principles of action

Konecta's Tax Policy is based on the following guiding principles:

- Konecta will comply with the tax obligations of the countries in which it operates, applying tax regulations in accordance with the criteria published and applied by the competent authorities, on the understanding that supporting the Treasury is a contribution to society.

- The Commercial Department shall inform the Tax Department of any new activities, operations and/or lines of business that it intends to initiate, so that the hypothetical tax implications that may arise can be studied.

- It shall establish internal control systems for tax-related processes to ensure compliance with tax obligations in accordance with the terms set out in the guidelines of this Policy.

- It will collaborate with the tax authorities in resolving any issues that may arise in relation to compliance with and application of tax obligations.

- If deemed necessary, the services of external advisors of recognised standing will be contracted in order to ensure Konecta's compliance with its tax obligations.

These principles of action respond to the impacts, risks and opportunities (IROs) arising from the applicable material issues: compliance and corporate ethics, communication and transparency with stakeholders.

Both employees and any third party 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 retaliation 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 the reporting parties.

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.

# Updating and revision

## Annex 5

The Fiscal Policy will be reviewed periodically or whenever necessary to adjust it to changes in the business model, the approval of new regulations or international best practices, ensuring its effectiveness and continued compliance.

NOTE: This Policy has been reviewed and 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 |
|---|---|---|---|---|---|
| 2 | 06/22/2021 | Finance<br>Organization & Procedures | Legal Affairs | Board of Directors | General Policy Review |
| 3 | 12/19/2022 | Finance<br>Organization & Procedures | Legal Affairs | Board of Directors | General Policy Review |
| 4 | 12/16/2025 | Finance<br>Organization & Procedures | Legal Affairs | Board of Directors | Alignment with legal requirements<br>Alignment with the new format and branding |

# Annex 6. Financing Policy

Corporate Policies 2025

# Table of contents

## ANNEX 6. FINANCING POLICY

# Purpose

## Annex 6

The objective of this Financing Policy (hereinafter, the “Policy”), which forms part of the Compliance Framework Policy of Konecta, a multinational group of companies specialising in the provision of digital customer management services and solutions (hereinafter, Konecta, the Company or the Firm), is to lay the foundations for prudent liquidity risk management, based on maintaining sufficient cash and financing availability, through an adequate amount of committed credit facilities in order to ensure optimal capacity to settle market positions.

This Policy is an extension of Konecta’s regulatory framework to establish a frame of reference and respond to the expectations of its stakeholders (employees, customers, partners and shareholders, investors, financial institutions, suppliers, public administration and regulatory bodies), ensuring scrupulous compliance with the laws and regulations in force in each country, its own requirements, and international standards. This Policy will be available on the corporate website (www.Konecta.com) to ensure that it can be consulted by all interested parties.

The objective of this policy is to guide decision-making regarding Konecta's financing, seeking a sustainable direction in this area. The aim is to manage capital in a way that ensures:

- Normal operation of business and long-term business continuity;
- Securing financing for new investments in order to maintain sustained growth over time;
- Maintaining an appropriate capital structure in line with the economic cycles that impact the business and the nature of the industry;
- Maximising the value of the Company by providing an adequate long-term return for shareholders.

To meet the above objectives, three fundamental pillars are considered:

## Financial strength:

- Credit metrics: efforts will be made to maintain them at levels appropriate to Konecta’s structure;
- Dividend policy: this must be conservative; adapting to the adequate maintenance of net equity and the cash requirements of the company distributing them;
- Liquid funds: these must be sufficient to cover short-term commitments.

## Optimal capital allocation:

- The parent company will ensure that the net debt of its subsidiaries remains at reasonable levels in accordance with approved investment projects;
- The channels of indebtedness must be the most convenient, considering all available options and conditions in terms of terms, rates, domestic or foreign financial institutions, direct indebtedness with securities placements in the market, diversification of sources, etc. The financial areas of the subsidiaries, under the control of the Corporate area, will plan their needs in a timely manner

to anticipate access to financial markets and obtain the best possible conditions;

- Transfers of financial resources to subsidiaries must follow market criteria.

## Strategic establishment of cash flows:

- Debt maturities must be well distributed over time and reasonably established with the cash flows generated by operations;
- The objective is to ensure that the currency in which the debt is denominated is appropriate to meet cash flows and minimise exchange rate fluctuations;
- Interest rate hedging to protect cash flows when required by the corporate area.

# Scope of application

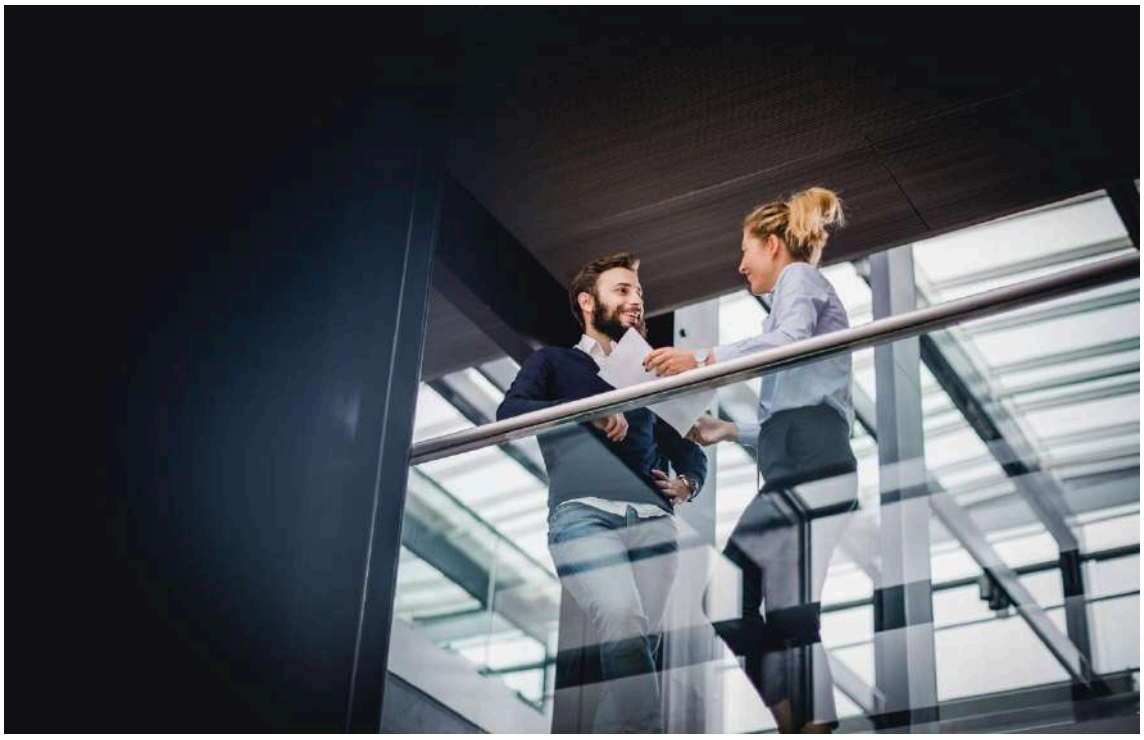
## Annex 6

This Policy falls within the scope of the Compliance Framework Policy and applies to all Konecta entities, backed by the company’s senior management.

Consequently, its content must be observed by all Konecta employees, regardless of their position or role within the organisation or their geographical location.

Given that many of Konecta's companies have their registered office outside the European Union, internal regulations will be adapted to the regulations of each State where necessary, respecting and ensuring compliance with the basic principles set out herein.

In the event of an unexpected event, occurrence, fact or change that individually or collectively could have a material adverse effect on the business, financial condition, assets, financial or operating results, cash flow and/or compliance with the contractual obligations of the Konecta Group, the guidelines established in this policy may be revised.



# General principles of action

## Annex 6

## Contingency plans

The following are mentioned as examples:

**Debt levels**
In the event that debt levels exceed those committed to by Konecta, one or more measures related to the following will be considered:

- Reduction of investments.
- Operational efficiencies.
- Dividend policy of Konecta entities
- Sale of assets.
- Capital increase.

Additionally, if any subsidiary presents adjusted metrics, measures such as the following may be considered:

- Capital contributions to the subsidiary.
- Modifications to the subsidiary's dividends.

**Maturities**
If the maturity profile does not fall within the agreed parameters, the following is recommended:

- Refinance debt.
- Prepay debt.

**Liquidity**
In the event that liquidity is lower than expected, the possibility of taking on debt, credit lines or other instruments that improve liquidity will be evaluated.

## Efficiency in funding sources

**Lower financial costs and better loan terms**
Debt financing channels must be the most efficient for each term, and they must be the most appropriate for meeting maturity distribution objectives. The company's subsidiaries will consider banking and public sources (where applicable) when making financing decisions.

In compliance with applicable legal requirements, certain Konecta entities may provide guarantees for debts incurred by subsidiaries and/or related companies, provided that this does not jeopardise the financial stability of the company and the indicators mentioned in this policy. Current guarantees will be included in the calculation of these indicators.

**Cash surplus and dividend policy in subsidiaries**
Unjustified cash surpluses may be withdrawn from certain subsidiaries and made available to the parent company to help finance or support business opportunities within the company, or to strengthen subsidiaries that may find themselves in a more vulnerable credit situation. Cash analyses will take into account the nature of each subsidiary and the respective investment plans, among other factors.

This will be achieved through the payment of dividends from the subsidiaries to the parent company, which will vary according to the situation and needs of each subsidiary at a given time. It is in Konecta's interest that the metrics of its main subsidiaries are in line with the requirements for being an investment-grade company.

The funds raised via dividends will be managed by the parent company and invested and/or distributed in accordance with the company's financial and dividend investment strategy.

Subsequently, the parent company could allocate resources for use by its subsidiaries as they request them, all subject to the approval of the corporate finance department.

The distribution of dividends or transfer of cash flows from a currency other than Konecta's functional currency will require a prior analysis of exchange rate hedging.

# Updating and revision

## Annex 6

The Financing Policy will be reviewed periodically or whenever necessary to adjust it to changes in the business model, the approval of new regulations or international best practices, ensuring its effectiveness and continued compliance.

NOTE: This Policy has been reviewed and 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 | 12/19/2022 | Finance<br>Organization & Procedures | Legal Affairs | Board of Directors | Initial edit |
| 2 | 12/16/2025 | Finance<br>Organization & Procedures | Legal Affairs | Board of Directors | Alignment with legal requirements<br>Alignment with the new format and branding |