

PRIVACY AND CONFIDENTIALITY FRAMEWORK POLICY

Madrid, June 22, 2021

Konecta





TABLE OF CONTENTS

- 1 PURPOSE
- 2 SCOPE OF APPLICATION
- 3 GENERAL PRINCIPLES OF ACTION
- 4 UPDATE AND REVIEW

This Privacy and Confidentiality Framework Policy sets out Konecta Group's (hereinafter Konecta, the Company, or the Organisation) basic principles with regard to the preventive and proactive responsibility for the principle of security and accountability to ensure privacy, and to the right fundamental right to the protection of personal data for which Konecta is responsible and accesses in its capacity as data processor during the performance of the services provided to its clients.

1.-PURPOSE

The purpose of this Privacy and Confidentiality Framework Policy (hereinafter the “Policy”) is to establish and disseminate Konecta’s basic and general rules on the protection of personal data, ensuring, in any case, strict compliance with the applicable legislation.

This policy is included within the corporate strategy for supporting information security, and includes the Information Security Policy, the Impact Assessment Guide, the Security Document, as well as the manuals and internal procedures existing in the Company on the matter.

Also, Konecta values and respects its own trade secrets as well as those belonging to its clients, and the rights of intellectual property. Confidentiality is considered a tool for managing our business competitiveness, protecting information ranging from business data relating to clients and suppliers to business plans and market studies or strategies, among others.

2.- SCOPE OF APPLICATION

This Policy is globally applicable to all Konecta entities and is endorsed by the General Management and the Board of Directors. Each member of the Company is responsible for promoting the principles and commitments contained herein while performing their duties.

Given that many of Konecta Group Companies have their registered office outside the EU, they shall adjust their internal regulations to the requirements and regulations of each State, respecting and safeguarding the basic principles herein outlined, with a view to continuously improve in the respect and protection of the information accessed.

3.- GENERAL PRINCIPLES OF ACTION

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

- Lawfulness, fairness and transparency.
- Purpose limitation.
- Data minimisation.
- Accuracy.
- Storage time limitation.
- Integrity and confidentiality.
- Information.
- Accountability
- Risk-based approach.

Konecta always informs stakeholders, with a clear and simple language, of the way the Company processes their data, particularly stressing that all personal data are confidential and stored under proper security measures, according to the characteristics thereof.

Special importance is given to the figure adopted by Konecta when providing its services, namely, that of data processor.

In this case, Konecta always provides sufficient guarantees to ensure that treatment is consistent with the duties imposed by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April, 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data, repealing Directive 95/46 / EC (GDPR), as well as the relevant Spanish legislation, namely, Organic Law 3/2018, of 5 December on Personal Data Protection and Guarantee of Digital Rights, to ensure protection of the rights of the person concerned, i.e., “the client of my client”.

Each country is required to comply with the maximum levels of European legislation, even when local regulation is laxer.

Konecta's obligations as data processor are:

- Always treating personal data following documented instructions from the controller (our client).
- Ensuring that authorised persons, i.e., Konecta employees processing personal data, have been trained on their obligations and agreed to respect the established security measures and confidentiality of treatment.
- Implementing all security measures necessary to prevent loss, theft, disclosure or misuse of personal data.
- Not using the data for any purpose other than the object of the contract.
- Assisting the controller to ensure compliance with the obligations under the regulation.
- Deleting or transferring back data once the provision of services ends.
- Providing the controller with all the necessary information to demonstrate compliance with the obligations set forth herein.
- Undertaking the responsibilities set out in the contract on the exercise of rights, assistance for conducting impact assessments, notifying security breaches, compliance with the duty to inform, etc.

Consequently, Konecta in its capacity as data processor, shall be responsible for complying with the obligations in the field of Data Protection set forth in the GDPR, and in any future regulation on this matter that may be enacted, developed or replaced in the future, with special attention to security measures and the collection of the consents that may be applicable to personal for processing purposes, for which Konecta shall always follow the specific instructions of the controller.

To ensure proper management and coordination of the personal data pertaining to Konecta and its clients, the Company has appointed a Data Protection Officer (DPO).

On any matter relating to the processing of personal data or privacy, you may send an e-mail to dpd@grupokonecta.com.

4.- UPDATE AND REVIEW

This Privacy and Confidentiality Framework Policy shall be reviewed and updated, where necessary, to adjust to the changes experienced by Konecta's business model, or to those which may be likely to occur in the company's field of action, or to those resulting from the adoption of rules of direct application, while ensuring its effectiveness and compliance.

This Policy is merely a summary of the key and general aspects concerning data protection. Konecta will make available the documents proving compliance with data protection rules to all stakeholders and clients for whom it acts as data processor.

This Policy has been re-reviewed, and its current wording was ratified by the aforementioned Board on June 22, 2021.