DATA PROTECTION AND PROCESSING POLICY

KinPOS CORPORATION

Issue date: 20/01/2025
Information classification: Internal and external

CONTENT

INTRODUCTION

This policy from KinPOS Corporation aims to guarantee the right of all individuals to know, update, and correct their personal information stored in its databases. It also sets forth the guidelines for the proper management of personal data, ensuring respect for the rights of privacy, intimacy, and good name.

KinPOS Corporation is committed to processing personal data in accordance with the principles of legality, purpose, freedom, accuracy, quality, transparency, access and restricted circulation, security, and confidentiality. All individuals who, within the framework of a contractual, commercial, labor, or other type of relationship, provide information to the company may exercise their rights of access, update, and correction in compliance with current regulations in the United States and in the countries where it operates.

To protect the personal data of customers, users, and employees, the company implements rigorous and effective security measures through cutting-edge technological tools that comply with the highest industry standards. In particular, KinPOS Corporation adheres to the most recent version of the Payment Card Industry Data Security Standard (PCI-DSS), which guarantees robust and reliable protection of cardholder information.

The purpose of adopting this policy is to ensure regulatory compliance and to address the inquiries and complaints of data subjects in a timely, clear, and efficient manner.

CONCEPTS AND DEFINITIONS

For the purposes of this policy, the following definitions apply:

- **Authorization:** The prior, express, and informed consent of the Data Subject to carry out the Processing of personal data.
- **Database:** An organized set of personal data that is subject to Processing.
- **Personal Data:** Any information that is linked to or can be associated with one or more specific or identifiable natural persons.
- **Sensitive Data:** Information that affects the Data Subject's privacy or whose improper use can lead to discrimination. For example: racial origin, political opinions, health data, or biometric data.
- **Private Data:** Data that, due to its intimate or private nature, is only relevant to the Data Subject.

- **Public Data:** Data that is not semi-private, private, or sensitive. Public data includes, among others, data related to the civil status of individuals, their profession or trade, and their status as a merchant or public servant. By its nature, public data can be contained in, among other things, public records, public documents, official gazettes and bulletins, and duly executed court rulings not subject to confidentiality.
- **Data Processor:** A natural or legal person, public or private, who, alone or in association with others, processes Personal Data on behalf of the Data Controller.
- **Authorized Entities:** KinPOS Corporation, as well as its nationally subordinated or associated branches and agencies.
- **Data Controller:** A natural or legal person who, alone or in association with others, decides on the Database and/or the Processing of the data.
- **Data Subject:** A natural or legal person whose Personal Data is subject to Processing.
- **Processing:** Any operation or set of operations on Personal Data, such as its collection, storage, use, circulation, or deletion. These definitions shall apply whether referred to in the singular or plural and shall be understood as modified when the law and/or applicable regulations and/or the interpretations of the competent authorities modify them.
- **Transfer:** The sending of personal data to a recipient who, in turn, is a Data Controller and is located inside or outside the country.
- **Transmission:** Processing of data that involves its communication inside or outside the national territory for the purpose of being processed by a Processor on behalf of the Controller.

PRINCIPLES

The Processing of personal data by Kinpos Corporation will be governed by the following principles:

- **Legality:** Data Processing is a regulated activity, subject to the law and other provisions that implement it in each country.
- **Purpose:** The collection of data must serve a legitimate purpose, which must be informed to the Data Subject in a prior and sufficient manner.
- **Freedom:** The collection of data can only be carried out with the prior, express, and informed consent of the Data Subject. Personal Data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that waives consent.
- **Truthfulness or Quality:** The information subject to Processing must be truthful, complete, accurate, up-to-date, verifiable, and understandable. The Processing of partial, incomplete, or misleading data is prohibited.

- **Transparency:** The Data Subject must be guaranteed the right to obtain, at any time and without restrictions, information about the existence of data concerning them.
- **Restricted Access and Circulation:** Personal data may not be available on the Internet or other mass dissemination media unless access is technically controllable and restricted to Data Subjects or authorized third parties.
- **Security:** The necessary technical, human, and administrative measures will be implemented to ensure the security of records, preventing their alteration, loss, unauthorized or fraudulent use, access, or consultation.
- **Confidentiality:** All individuals involved in the Processing of Personal Data are obligated to guarantee the confidentiality of the information, even after their relationship with any of the tasks involved in the Processing has ended.

DATA CONTROLLER

NAME OR BUSINESS NAME: KinPOS Corporation

DOMICILE AND ADDRESS: A company legally incorporated under the laws of the United States of America, domiciled at 3350 SW 148th Ave. Suite 110, Miramar, FL 33027

EMAIL ADDRESS: privacy@kinpos.com

REGULATORY FRAMEWORK

This policy was prepared taking into account the provisions contained in **U.S. legislation** and is committed to complying with the data protection laws of the jurisdictions where it operates, including, but not limited to:

Country	Applicable Law	Control Authority	Data Subject Rights	Response Time
USA	CCPA / NIST Privacy Framework	FTC	Access, rectification, deletion, portability	Varies by state
Colombia	Law 1581 of 2012, Decree 1377	SIC	To know, update, rectify, delete, revoke	15 business days
Mexico	Federal Law on the Protection of Personal Data	INAI	ARCO (Access, Rectification, Cancellation, Opposition)	20 business days
Peru	Law 29733	ANPD (MINJUS)	Access, rectification, cancellation, opposition	20 business days

Costa Rica	Law 8968	PRODHAB	Access, rectification, cancellation	10 business days
Panama	Law 81/2019	ANTAI	Access, rectification, cancellation	10 business days
El Salvador	Sectoral regulations	Consumer Protection Agency	Access, update, deletion (limited)	Varies by sector
Nicaragua	Law 787	MHCP	Access, rectification, cancellation, opposition	15 business days
Caribbean	Local regulations inspired by GDPR	Local authorities	Access, rectification, deletion, portability	Approx. 30 days

Table: 1 / Regulatory Framework

SCOPE OF APPLICATION

This Policy is mandatory and of strict compliance for:

- Directors.
- Shareholders, statutory auditors, and other individuals with whom a legal relationship of a statutory nature exists.
- Suppliers or strategic partners who store and process information and/or databases.
- Contractors, as well as natural or legal persons who provide services under any contractual arrangement that involves data processing.
- Public or private individuals in their capacity as personal data users.
- Other persons as determined by law.

In this context, the Data Protection and Processing Policy (hereinafter referred to as the "Policy") is issued, which regulates the management of information contained in databases. This data belongs to natural and legal persons who are the data subjects of the information, who have granted their authorization for the respective processing, in accordance with corporate guidelines and the provisions of this document.

AUTHORIZATION

The collection, storage, use, circulation, and in general, the Processing of Personal Data contained in the databases require the free, prior, express, and informed consent of the Data Subjects.

KINPOS CORPORATION, in its capacity as the Data Controller, has provided the necessary mechanisms to obtain Authorization from Data Subjects prior to the collection of their data, ensuring in all cases that it is possible to verify and prove that said Authorization was granted.

Personal information will remain in the databases only for the time necessary to fulfill the authorized purposes, unless the Data Subject requests its deletion.

Form and Mechanisms for Granting Authorization

Authorization can be granted in a physical or electronic document, a data message, on the Internet, a website, or also verbally or by telephone, or in any other format that allows for its subsequent verification; or through an unequivocal action by the Data Subject that allows for the reasonable conclusion that they granted the authorization; or through a suitable technical or technological mechanism by which it can be unequivocally concluded that, without having obtained the Data Subject's consent, the data would never have been collected and stored in the Database.

The consented authorization procedure ensures that the Data Subject has been informed that their personal information will be collected and used for specific and known purposes in accordance with this Policy and the corresponding Privacy Notice, as well as their right to request access, update, rectification, and deletion of their Personal Data at any time, through the mechanisms made available to them by KINPOS CORPORATION. This is to enable the Data Subject to make informed decisions regarding their Personal Data and to control the use of their personal information.

The Authorization is a statement that informs the Data Subject of the Personal Data about:

- Who is collecting their personal information
- What is being collected (the data gathered)
- The purpose for which the data is collected (the purposes of the Processing)
- How to exercise the rights of access, correction, update, or deletion of the Personal Data provided
- To inform the Data Subject that, in the case of Sensitive Data (if applicable), they are not obligated to authorize its Processing

PRIVACY NOTICE

A Privacy Notice is a physical, electronic, or any other form of document that is made available to the Data Subject to inform them about how KINPOS CORPORATION will Process their Personal Data, before the collection of that Personal Data is authorized.

Through this document, the Data Subject is informed about the existence of the Information Processing Policies that will apply to them, how to access those policies, and the characteristics of the intended Processing of the Personal Data.

Minimum Content of the Privacy Notice

The Privacy Notice must contain at least the following information:

- The identity, address, and contact information of the Data Controller.
- The type of Processing the data will undergo and its purpose.
- The rights of the Data Subject.
- The general mechanisms provided by the Data Controller for the Data Subject to learn about the information Processing policy and any substantial changes to it or the corresponding Privacy Notice. In all cases, it must inform the Data Subject how to access or consult the information Processing policy.
- Notwithstanding the above, when Sensitive Personal Data is collected, the Privacy Notice will expressly state the optional nature of the response to questions concerning this type of data.

TYPES OF INFORMATION COLLECTED

KinPOS Corporation may obtain and process personal data from various sources, including but not limited to, the use of its website, the acquisition of its products and services, personnel selection processes, and the interaction with its payment systems. The information collected includes, among others:

- **Transactional and Financial Data**: Information related to payment orders or transfers made using cards, electronic wallets, or other payment methods may be collected, including the amount, date, time of the transaction, and the merchant's business category. Information associated with credit or debit cards and bank accounts may also be collected. All of this information will be processed under strict protocols and controls defined within the Information Security System to ensure its **confidentiality, integrity, and availability**, protecting it from unauthorized access, improper use, or any form of **breach**.
- **Technical and Usage Data**: Information about the mobile device (model, operating system, IP address), geographical location, and the use of cookies on the website.
- **Employee and Applicant Data**: Information related to date and place of birth, nationality, work experience, marital status, academic history, personal references, and disciplinary and judicial records.

- **Personal and Contact Data**: Full name, type and number of identification, email address, phone number, among others.
- **Video Surveillance Data**: Data obtained through video cameras at offices and facilities for security and control purposes.

PURPOSES OF DATA PROCESSING

The personal data collected will be used only for the purposes authorized by its **data subjects**, which vary according to the stakeholder group they belong to:

- **Clients, Users, and Financial Institutions:** To manage pre-contractual, contractual, and post-contractual activities; to develop marketing, sales, and promotional actions; to handle procedures, inquiries, and claims; and to understand and evaluate credit and commercial behavior.
- **Suppliers and Partners:** To carry out the onboarding process and verify commercial and reputational backgrounds for money laundering and FT (SARLAFT/ AML/CTF + LEFT + LAFT + FATCA + UBO).
- **Applicants and Employees:** To manage selection processes, formalize the employment relationship (social security, payments, benefits), and comply with applicable legal regulations.
- **Shareholders and Board Members:** To manage the shareholder registry book, issue calls for meetings, and manage the risk of money laundering and corruption.
- **Facility Security:** To control and identify access to facilities using registration and video surveillance mechanisms, the information from which may be used as evidence in judicial or administrative proceedings.
- **Regulatory Compliance:** To address applicable legal, tax, financial, and regulatory provisions.
- **Technological Support and Electronic Transactions:** To guarantee the correct operation of the services provided and the security of transactions.
- **Corporate Communication:** To establish contact with the data subjects.

RIGHTS AND DUTIES

This section details your rights as a data subject over your personal data, as well as the responsibilities and obligations that KINPOS Corporation assumes to guarantee its ethical and secure use.

Below, we describe your rights and the duties that govern our actions in handling your information.

Rights of the Data Subjects

Data subjects have the following rights over their personal data:

- To know, update, and rectify their personal data.
- To request a copy of the authorization granted for the processing of their data.
- To revoke the authorization and request the deletion of their data when constitutional and legal principles, rights, and guarantees are not respected.
- To access their personal data that has been processed, free of charge. The company will provide contact channels for the data subject to exercise their rights.

Duties of the Personal Data Controller

Kinpos Corporation will, at all times, bear in mind that personal data is the property of the data subject. Therefore, it will use the data only for the purposes for which it is duly authorized, and will comply with the following duties:

- To guarantee the full and effective exercise of the right to habeas data.
- To retain a copy of the authorization granted by the data subject.
- To inform the data subject about the purpose of the collection and their rights.
- To maintain the information under the necessary security conditions to prevent its alteration, loss, or unauthorized access.
- To guarantee that the information provided is truthful, complete, accurate, up-to-date, verifiable, and understandable.
- To update the information by communicating any new developments in a timely manner.
- To rectify the information when it is incorrect.
- To provide only the data for which processing has been previously authorized.
- To demand respect for the security and privacy conditions of the information at all times.
- To process inquiries and claims within the established timeframes.
- To inform when the information is being disputed by the data subject.
- To inform about the use of the data when the data subject requests it.

- To notify the data protection authority of any violation of security codes or risks in the administration of the information.
- To comply with the instructions and requirements issued by the authorities.

Kinpos Corporation guarantees and requires the confidentiality of private, sensitive, or minor's personal data from every person who is involved in any phase of its processing.

PROCEDURE FOR EXERCISING RIGHTS

KinPOS is committed to protecting personal data, ensuring that **data subjects** can exercise their rights as owners of their information quickly and securely.

Here's the channel that **data subjects** or their legal successors should follow to submit inquiries or claims regarding the **processing** of their data. By using this procedure, we ensure that every request is handled transparently and within the timeframes established by law, guaranteeing your right to privacy and control over your personal information.

- **Email:** privacy@kinpos.com

To process a request, it must contain at least the following information:

- The full name and identification of the **data subject**.
- A clear description of the facts leading to the request.
- A physical or electronic address to receive the response.
- Relevant documents and evidence to support the request (if applicable).

Response Times

To ensure a timely response within the established timeframes, please refer to Table 1 Regulatory Framework on pages 5 and 6.

- **Inquiries:** The maximum period to respond to an inquiry is ten (10) business days from the date of its receipt.
- **Claims:** The maximum period to handle a claim is fifteen (15) business days, counted from the day after the date of its receipt.

INTERNATIONAL DATA TRANSFER

Kinpos Corporation, as a company with global operations, may transfer personal data to its affiliates, branches, and partners located in different countries. This transfer will be carried out exclusively for the purposes described in this policy and in compliance with the following guidelines:

- Data Subject's Authorization: By accepting this policy, the data subject provides prior, express, and informed authorization for the transfer and/or transmission of their personal data to other jurisdictions.
- Security Measures: Kinpos will implement technical, organizational, and contractual measures to ensure an adequate level of data protection in the receiving country, including, where applicable, the use of mechanisms approved by data protection authorities, such as those mentioned in the international compliance section.

INTERNATIONAL COMPLIANCE

As a U.S.-based company with operations in multiple countries, Kinpos Corporation is committed to ensuring strict compliance with the applicable data privacy laws, regulations, and standards of the different nations and economic blocs where it operates. In essence, one of our main objectives is to ensure that personal information has a consistent and robust level of protection, regardless of where it is transferred, processed, or stored globally.

INFORMATION SECURITY

Information Security Policies

At Kinpos Corporation, the commitment is to protect the information of our clients, suppliers, employees, contractors, and other stakeholder groups. To achieve this, the company has implemented a robust Information Security Policy that adheres to applicable regulations and the most rigorous industry standards.

Regulatory Framework and Industry Standards

Kinpos está dedicada a cumplir con todas las leyes y regulaciones en materia de seguridad de la Kinpos is dedicated to complying with all laws and regulations concerning information security and cybersecurity. Its internal policies are supported by the implementation of controls based on recognized global standards, such as:

- **PCI-DSS** to ensure the security of card payment data.
- **Information Security Management System (ISMS)** based on industry standards.

Responsibility and Information Disclosure

While Kinpos implements the most advanced security measures to protect its systems and databases, it is not liable for the interception, misuse, or breach of these by unauthorized or malicious third parties. In the event of a breach, Kinpos will act in accordance with the law and inform the relevant authorities as soon as it becomes aware of the incident.

Third-Party Commitment

All third parties Kinpos Corporation collaborates with, including, but not limited to, contractors, consultants, and suppliers, are obligated to adhere to its Information Security and Cybersecurity Policies, as well as the strict security protocols the company applies in all its processes. Additionally, they are required to comply with the policies and procedures of the clients to whom Kinpos provides services.

Any contract with a third party that involves handling information or personal data includes a confidentiality agreement that details their obligations to ensure the protection, care, and preservation of the information's confidentiality, integrity, and availability. These agreements are integrated into Kinpos' information security system to prevent any alteration, loss, or unauthorized access.

Implementation of Security Measures

KINPOS CORPORATION will maintain mandatory security protocols for all personnel who have access to personal data and information systems.

The procedure must consider, at a minimum, the following aspects:

- Training for the data controller of databases on the proper handling of both physical and automated information that resides with the company, following the parameters established by law, as well as for the protection and security of the data.
- Training for all personnel entering the company on the Personal Data Processing Policy and the security mechanisms and protocols for processing this data.
- The scope of application for the procedure, with a detailed specification of the protected resources.
- The activities and responsibilities of the service and/or role.
- The structure of the Personal Databases and a description of the information systems that process them.
- A procedure for notification, management, and response to incidents.

- Procedures for making backup copies and for data recovery.
- Periodic controls that must be performed to verify compliance with the provisions of the security procedure being implemented.
- Measures to be adopted when a medium or document is transported, discarded, or reused.
- The procedure must be kept up-to-date at all times and must be reviewed whenever relevant changes occur in the information system or its organization.
- The content of the procedure must be adapted at all times to the current provisions regarding Personal Data security.

EFFECTIVENESS AND CHANGE CONTROL

This Data Protection and Processing Policy is effective as of its publication and may be modified at any time to adapt to new legal or internal provisions. Changes will be communicated via the website https://kinpos.com/us/, and **Data Subjects** must review it periodically to stay informed of any updates.

CODE	VERSION	DATE	CHANGE DESCRIPTION
POL-PTD- 01	1	04/18/2023	Initial document
POL-PTD- 01	2	01/20/2025	Comprehensive document update