



Akua's Data Privacy Policy

Policy Owner: Head of Legal - Lina Oviedo

Effective Date: September 12, 2024

Overview

This policy establishes the general guidelines that Akua will apply to the processing of personal data for which Akua acts as Data Controller and/or as Data Processor. As a company specializing in transactional data processing for acquirers, Akua is committed to complying with international and local data protection regulations.

Scope of Application

This policy applies to all activities involving the collection, storage, use, circulation, and deletion of personal data, particularly transactional data, conducted by Akua, both within and outside Colombia. Akua acts as a data processor for personal data provided by acquirers and aggregators and complies with all obligations derived from the GDPR and Colombian regulations.

Definitions

- **Personal Data:** Information linked to or that can be associated with one or more identified or identifiable natural persons.
- **Transactional Data:** Information related to financial transactions, such as payment data, purchase histories, bank account numbers, BIN numbers, and any other data generated during the acquisition of goods or services.
- **Sensitive Data:** Information that affects the data subject's privacy or that, if misused, could lead to discrimination, such as racial origin, political orientation, religious beliefs, biometric data, etc.
- **Data Subject:** The natural person whose personal data is subject to processing.
- **Data Controller:** The natural or legal person who decides on the database and data processing. In this case, acquirers and aggregators are the data controllers. Akua only acts as a Data Controller for the personal data of its employees, contractors, suppliers, and customers.
- **Data Processor:** The natural or legal person who processes data on behalf of the data controller. In this case, Akua acts as a data processor for personal data provided by acquirers and aggregators for transactional data.

Principles

In compliance with the General Data Protection Regulation (GDPR), Akua adheres to the following principles:



- **Lawfulness, Fairness, and Transparency:** Akua ensures that personal data is processed lawfully, fairly, and transparently in relation to data subjects.
- **Purpose Limitation:** Data will be collected for specified, legitimate purposes and will not be processed in a manner incompatible with those purposes.
- **Data Minimization:** Akua ensures that the personal data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- **Accuracy:** Personal data will be accurate and kept up to date when necessary.
- **Storage Limitation:** Personal data will be retained in a form that allows identification of data subjects only for as long as necessary for the purposes of processing.
- **Integrity and Confidentiality:** Akua implements appropriate technical and organizational measures to ensure the security of personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

Obligations

Akua assumes the following specific obligations regarding the processing of personal data:

- **Obtaining Prior and Express Consent:** Before collecting or processing personal data, Akua must obtain the prior, express, and informed consent of the data subjects, except in cases authorized by law or where Akua acts as a data processor, subject to the agreements made with the data controller.
- **Registration:** Akua will comply with local laws and rules on personal data protection and will register its databases with the corresponding registry according to the jurisdiction and before the competent authority.
- **Data Subjects' Rights:** Akua guarantees that data subjects can exercise their rights to access, update, rectify, delete, and revoke consent regarding their personal data.
- **Data Retention:** Personal data will only be retained for as long as necessary to fulfill the purposes of processing, respecting the retention periods established by Colombian law.
- **Security Measures:** The necessary technical and organizational measures will be implemented to ensure the security of personal data, as established in the Information Security Policy.
- **International Data Transfers:** Akua may transfer data to other jurisdictions, including the United States of America, provided that the applicable local provisions in the jurisdiction where the personal data is held are complied with, and ensure that the recipient countries provide adequate levels of data protection.

Purposes of Transactional Data Processing

As a data processor, Akua will use transactional data for the following purposes:



- **Transaction Processing:** To process data generated in payment transactions and other financial services associated with acquirers and aggregators.
- **Fraud Prevention:** To implement risk analysis measures to detect and prevent fraudulent activities.
- **Regulatory Compliance:** To comply with the legal and regulatory obligations imposed by financial and data protection authorities.
- **Service Improvement:** To analyze data to optimize and improve the services offered to acquirers and aggregators, within the framework of authorized purposes.

Security Measures

Akua will implement the necessary security measures to protect transactional data from unauthorized access, loss, alteration, or improper disclosure. These measures include, but are not limited to, the following and those established in the Information Security Policy:

- **Data Tokenization:** All transactional data will be tokenized, meaning that sensitive information will be replaced with a unique identifier (token) that has no value outside Akua's tokenization system.
- **Controlled Access:** Tokenized data will only be accessible through cryptographic keys and authorization established in Akua's cybersecurity procedures.
- **Data Encryption:** In addition to tokenization, data will be encrypted during storage and transmission, using robust encryption standards.
- **Regular Audits:** Periodic audits of security systems are conducted to ensure compliance with regulations and to identify and mitigate vulnerabilities.

International Data Transfers

In its role as a data processor, Akua may transfer transactional data to other jurisdictions, including the United States of America. Such transfers will be carried out in compliance with applicable regulations in the jurisdiction where the transactional data is located. Akua will ensure that international transfers are conducted under adequate security standards and with protection equivalent to that required in the jurisdiction where the data is located or from which the transactional data will be transferred.

Procedure for Exercising Rights

Data subjects may exercise their rights by submitting a written request to Akua at the email address Dataprivacy@akua.la Akua will respond within the timeframes established by law.

Policy Modifications

Akua reserves the right to modify this policy at any time. Any changes will be communicated to the data subjects through registered contact channels and/or via the company's website.



Data Controller

Akua is the data processor of the personal data provided by acquirers and aggregators. Any inquiries or claims related to data processing may be directed to Dataprivacy@akua.la

This policy is effective as of its publication date and will be available to data subjects at any time through the website www.akua.la

Version	Date	Description	Autor	Approval
1.0	September 12, 2024	Primera Versión	Lina Oviedo	Juan Jose Behrend