Personal Data Management Policy

EFFECTIVE: JUNE 16, 2025

Index

Name

Position

Signature

Date

Prepared by:

Jorge Navarro / Sebastián Natera

Attorney / CEO

Jorge Navarro / Sebastián Natera

May 16, 2025

Reviewed by:

Jorge Navarro / Sebastián Natera

Attorney / CEO

Jorge Navarro / Sebastián Natera

June 16, 2025

Approved by:

Jorge Navarro / Sebastián Natera

Attorney / CEO

Jorge Navarro / Sebastián Natera

June 16, 2025

---

1. Objective

The purpose of this Policy is to establish guidelines for the management of personal data and for obtaining consent from Data Subjects for the processing of their personal data, as an integral part of the internal processes of **KADU CARE GROUP, S.A. DE C.V.** (“KADU CARE”) and its respective **stakeholders** (clients, suppliers, job candidates, and employees).

---

2. Scope

This Policy applies to all personal data held by KADU CARE that is processed by its personnel in operational, business, and activity-related processes.

It also applies to entities that collaborate with KADU CARE, whether acting as data processors or controllers, and that process personal data on behalf of KADU CARE.

This Policy applies to all stages of the personal data lifecycle, including generation, distribution, storage, processing, transfer, transmission, consultation, and final disposal. It also applies to all stages of the lifecycle of systems that process such data, including analysis, design, development, implementation, maintenance, and destruction.

---

3. Definitions and Abbreviations

Privacy Notice

A physical, electronic, or any other format document generated by the data controller (KADU CARE), made available to the Data Subject prior to the processing of personal data, in accordance with the Federal Law on the Protection of Personal Data and other applicable regulations, under the supervision of the Ministry of Anti-Corruption and Good Governance (SABG).

Consent

The manifestation of the Data Subject's will by which they authorize the processing of their personal data. Consent must be obtained in accordance with the type of data processed.

Express Consent

Consent given verbally, in writing, electronically, optically, through recordings, or by any other technology or unequivocal means.

Implied Consent

Consent is considered implied when the Privacy Notice has been made available to the Data Subject and the latter does not express opposition.

Personal Data

Any information concerning an identified or identifiable natural person, such as name, address, age, telephone number, email address, signature, photograph, tax ID, etc.

Financial/Patrimonial Personal Data

Data that allow inference of a person's financial situation, including bank balances, account numbers, investment accounts, movable and immovable assets, tax information, credit history, income, expenses, insurance policies, salaries, and banking card numbers.

Sensitive Personal Data

Personal data that affect the most intimate sphere of the individual or whose misuse may give rise to discrimination or pose a serious risk, such as health data, diseases, union affiliation, criminal history, religion, or sexual preference.

ARCO Rights

Rights of Access, Rectification, Cancellation, and Opposition that the Data Subject may exercise regarding the processing of their personal data.

Dissociation

A procedure by which personal data cannot be associated with a Data Subject, nor allow identification through its structure, content, or level of aggregation.

Processor

A natural or legal person that processes personal data on behalf of KADU CARE, such as insurers, banks, law firms, audit firms, and AI service providers.

Publicly Available Sources

Sources accessible to the public, including:

- Electronic, optical, or other technological media intended to provide public information;
- Telephone directories;
- Official journals, gazettes, or bulletins;
- Social media platforms.

Access must not be restricted by law or beyond the payment of a fee.

Stakeholders

Individuals or legal entities that have an interest in or are affected by KADU CARE's activities.

Direct Collection of Personal Data

When personal data is obtained directly from the Data Subject by electronic, optical, visual, auditory, or other technological means.

Indirect Collection of Personal Data

When personal data is obtained through public sources or by transfer or disclosure.

In-Person Collection of Personal Data

When data is collected in the physical presence of the Data Subject and the Controller or its representative.

Data Protection Officer (DPO)

The highest authority within KADU CARE responsible for personal data protection compliance.

Transfer

The communication of personal data between the Controller and the Processor, within or outside Mexico.

Controller

The natural or legal person who decides on the processing of personal data—in this case, KADU CARE.

Personal Data Security Management System (PDSMS)

A management system designed to establish, implement, operate, monitor, review, maintain, and improve personal data protection, based on risk assessment and principles of legality, consent, information, quality, purpose, loyalty, proportionality, and accountability under applicable law.

---

4. Responsible Party

The Data Protection Officer is responsible for keeping this Policy updated and ensuring compliance.

KADU CARE appoints **RAJAN SAPKOTA** as Data Protection Officer.

Phone: +1 (236) 978-1339

Email: rajan@kaducare.com | info@kaducare.com

---

5. Related Documents

- Comprehensive Privacy Notice
- Simplified Privacy Notices

---

6. Sanctions

This Policy forms part of KADU CARE's Internal Work Regulations. Violations by employees may result in disciplinary measures, without prejudice to civil, administrative, or criminal liability.

Non-compliance by KADU CARE suppliers may result in termination of the corresponding agreement and potential civil, administrative, or criminal liability.

---

7. Policy

KADU CARE is committed to managing personal data lawfully and obtaining consent from Data Subjects. This Policy ensures compliance with the Mexican Federal Personal Data Protection Law under the supervision of the SABG and alignment with HIPAA (USA), PIPEDA (Canada), and GDPR (EU).

KADU CARE acts as a support tool. Compliance with NOM-024-SSA3-2012 regarding Electronic Health Records (EHR) remains the sole responsibility of the healthcare provider or institution.

---

8. Principles of Personal Data Protection

KADU CARE personnel commit to:

- Obtaining consent from Data Subjects or their legal representatives and informing them of processing purposes through the Privacy Notice.

- Ensuring lawful and non-deceptive data collection.
- Maintaining data accuracy and quality.
- Limiting processing to necessary timeframes and purposes.
- Deleting or blocking data once purposes are fulfilled.
- Collecting only data necessary for stated purposes.
- Preventing unauthorized disclosure of personal data.
- Preventing unauthorized copying or reproduction of personal data.
- Ensuring third parties receiving data adhere to confidentiality obligations.
- Implementing administrative, technical, and physical security measures.
- Restricting data access according to authorization levels.
- Identifying the full lifecycle of personal data.
- Maintaining updated personal data inventories.
- Addressing Data Subject rights requests promptly.
- Developing and maintaining a Personal Data Security Management System (PDSMS).
- Applying Privacy by Design and Privacy by Default principles, including Data Protection Impact Assessments (DPIAs) when high-risk processing is involved (e.g., AI in healthcare).
- Conducting annual internal or external audits of information systems.
- Maintaining an Incident Response Plan including detection, containment, analysis, notification, and remediation within 72 hours when required.

KADU CARE recognizes international standards such as GDPR, PIPEDA, and HIPAA, including data portability, processing restriction, and accountability principles.

---

9. Collection of Personal Data and Consent

When collecting personal data:

- The Privacy Notice must be made available at all points of collection, including:
    - KADU CARE website
    - Data collection forms
    - Training enrollment
    - Recruitment processes
    - Vendor onboarding

Types of data include:

- Identification data
- Location data
- Financial data
- Banking information
- Authentication data
- Legal data
- Health data
- Sensitive ideological or belief data

Consent exceptions include:

- Legal requirements
- Publicly available data
- Prior anonymization
- Contractual obligations

- Medical emergencies
- Health care provision under professional secrecy
- Authority orders

Relevant KADU CARE departments include HR, Finance, Sales, IT, Administration, and Procurement.

Consent must be obtained before or at the time of data collection. If obtained physically, documents must be securely stored. If obtained digitally, IT must ensure secure storage.

Only necessary data must be collected. Any uncertainty must be resolved with the Data Protection Officer.

Data obtained from public sources requires Privacy Notice disclosure upon first contact.

Before receiving data from third parties, contractual safeguards must be in place.

---

10. Communication

This Policy must be known by all personnel involved in personal data processing.

KADU CARE will maintain a confidential whistleblowing channel allowing employees, contractors, or third parties to report incidents or violations anonymously. Reports will be managed by the Data Protection Officer with confidentiality and due process.

---

11. References

- Federal Law on the Protection of Personal Data (Mexico – SABG)
- HIPAA (United States)
- PIPEDA (Canada)
- GDPR (European Union)

KADU CARE recognizes rights to data portability and restriction of processing in accordance with GDPR and PIPEDA.

12. Change History

Version	Change Description	Change Request No.

In the event of future regulatory changes in Mexico, references herein shall be understood as referring to the authority legally replacing the current one.