



+27 10 142 1480

info@kandua.com

www.kandua.com

Head Office: 9 Somerset Rd, Green Point, Cape Town, 8001

Kandua Privacy Policy

Kandua Privacy Policy

Kandua Privacy Policy

Policy Overview

Kandua Privacy Policy Statement

Alignment with Santam Group Privacy Policy

Purpose and Objectives

Scope and Applicability

Legal and Governance Framework

Alignment with POPIA, GDPR (if applicable), and other data protection laws

Group Governance and Oversight

Roles and Responsibilities

Privacy Principles

Accountability

Lawful and Fair Processing

Purpose Specification

Data Minimisation and Processing Limitation

Transparency and Openness

Further Processing and Compatibility

Data Quality and Accuracy

Security Safeguards

Data Subject Participation and Access

Categories of Personal Information

Personal Information Definition

Special Personal Information

Information of Children and Minors

Employee and Contractor Information

[Client and Partner Information](#)

[Cross-Reference with PAIA Manual](#)

[Collection and Processing of Personal Information](#)

[How Information is Collected](#)

[Purpose of Collection and Processing](#)

[Lawful Bases for Processing](#)

[Processing Limitation](#)

[Processing of Special Categories](#)

[Information Disclosures](#)

[Privacy Notice and Transparency Requirements](#)

[Mandatory Disclosures in Privacy Notices](#)

[Use and Sharing of Information](#)

[Intra-Group Information Sharing](#)

[Disclosure to Authorised Third Parties \(Operators\)](#)

[Operator Agreements and Due Diligence](#)

[Disclosure to Competent Authorities](#)

[Third-party Data Processors and Vendors](#)

[Prohibition on Sale of Personal Information](#)

[Cross-border Transfers](#)

[Conditions for International Transfers](#)

[Safeguards and Legal Justifications](#)

[Cloud Storage and Data Residency Considerations](#)

[Record-keeping for Cross-border Processing](#)

[Security Safeguards and Controls](#)

[Technical and Organisational Measures](#)

[Encryption and Access Control](#)

[Incident Management and Breach Reporting](#)

[Third-party Security Compliance](#)

[Physical and Cybersecurity Controls](#)

[Employee Responsibilities and Breach Escalation](#)

[Data Storage and Retention](#)

[Retention Periods](#)

[Destruction and De-identification](#)

[Archiving for Statistical, Research or Legal Purposes](#)

[Restriction of Processing after Purpose Fulfilment](#)

[Direct Marketing](#)

[Consent and Opt-in/Opt-out Requirements](#)

[Communication Preferences and Records](#)

[Restrictions on Unsolicited Communications](#)

[Rights to Object to Marketing](#)

Automated Decision-making and Profiling

[Conditions for Automated Decisions](#)

[Right to Human Intervention](#)

[Transparency in Logic Used](#)

[Protection of Legitimate Interests](#)

Data Subject Rights

[Right of Access](#)

[Right to Rectification or Correction](#)

[Right to Erasure](#)

[Right to Restrict Processing](#)

[Right to Object](#)

[Right to Data Portability](#)

[Right to Lodge Complaints](#)

Procedure for Access Requests

[PAIA Compliance and Access Request Process](#)

[Verification and Response Timelines](#)

[Request Forms and Channels](#)

[Fees and Exceptions](#)

Complaints and Enquiries

[Internal Complaints Handling Procedure](#)

[External Escalation](#)

[Dispute Resolution Process](#)

Information Officer Contact Details

[Information Officer](#)

Deputy Information Officer

[Physical and Postal Address](#)

[Telephone and Email Contact](#)

[Link to Online PAIA Manual](#)

Cookies and Digital Tracking

[Use of Cookies and Similar Technologies](#)

[Purpose](#)

[User Control and Opt-out Options](#)

Policy Implementation and Enforcement

[Compliance Monitoring and Reporting](#)

[Staff Training and Awareness](#)

[Disciplinary Action for Non-compliance](#)

[Annual Review and Updates](#)

[Record of Amendments](#)

[Definitions and Interpretation](#)

[Core Definitions](#)

[Reference to Applicable Legislation](#)

Kandua Privacy Policy

Policy Overview

Plus Ecosystem Ventures (Pty) Ltd (t/a "Kandua") is committed to ensuring that all personal information is processed lawfully, fairly, and transparently, in alignment with the constitutional right to privacy, the **Protection of Personal Information Act, No. 4 of 2013 (POPIA)**, and the **Promotion of Access to Information Act, No. 2 of 2000 (PAIA)**.

This Privacy Policy outlines Kandua's approach to the collection, processing, protection, and management of personal information. It serves as a statement of intent and accountability to uphold the highest standards of data privacy and information security within all Kandua business operations and ecosystems, including the **Marketplace, Insurance, Partnership, and Service Provider (Pro)** ecosystems.

Kandua aligns itself with the **Santam Group Privacy Policy** and related governance frameworks to ensure consistent application of privacy principles across the broader group structure, while adopting operational practices suitable to Kandua's platform, customer base, and technology infrastructure.

This Policy complements Kandua's **PAIA Manual**, which provides details on how members of the public may request access to information and outlines Kandua's records, information categories, and data subject processing activities.

Kandua Privacy Policy Statement

Kandua is committed to ensuring that Personal Information is at all times processed in a fair, lawful, and responsible manner, and in full compliance with applicable legislation, including the constitutional right to privacy. Kandua strives to uphold an appropriate level of security and confidentiality in respect of all Personal Information under its control or custody. This includes, but is not limited to, information relating to customers, service providers, business partners, and employees. In carrying out its activities, Kandua seeks to protect the integrity, accuracy, and confidentiality of Personal Information, ensuring that it is processed only for legitimate business purposes and safeguarded against unauthorised access, disclosure, or misuse.

Alignment with Santam Group Privacy Policy

As part of the Santam Group, Kandua aligns itself with and is guided by the **Santam Group Privacy Policy**. This means that Kandua's data protection and privacy practices are consistent with the Group's overarching principles, standards, and obligations. By doing so, Kandua ensures that its approach to data privacy is not only compliant with South African law (including the Protection of Personal Information Act, 2013), but also harmonised with the broader privacy governance framework of the Santam Group.

Purpose and Objectives

The purpose of this Privacy Policy is to:

1. **Establish governance and accountability** for the responsible collection, processing, and safeguarding of personal information within Kandua's operations and systems.
2. **Ensure compliance** with POPIA, PAIA, and all other applicable data protection, consumer protection, and financial sector laws.
3. **Promote transparency** by informing data subjects how and why Kandua collects, uses, shares, and retains personal information.
4. **Protect the rights of data subjects**, including customers, service providers, partners, employees, and other stakeholders, by outlining the measures

Kandua employs to maintain confidentiality, integrity, and lawful processing of information.

5. **Provide a framework for information sharing** across Kandua's internal teams, partners, and authorised third parties in a manner consistent with the **Santam Group Privacy Principles**, binding corporate rules, and contractual obligations.
6. **Guide employees and management** on their obligations in handling personal information and maintaining appropriate security controls and reporting mechanisms in the event of any data incident or breach.

Through this policy, Kandua seeks to demonstrate a culture of privacy-by-design and to embed ethical information management practices across all operational, digital, and partner interfaces.

Scope and Applicability

This Privacy Policy applies to:

- All **personal information** processed by Kandua, whether in physical or electronic form, throughout the entire **information life cycle** — from initial collection and use to storage, transfer, archival, and deletion.
- All **Kandua business units, systems, products, and platforms**, including any connected applications used to manage customer and service provider data.
- All **data subjects** whose personal information is collected or processed by Kandua, including:
 - Homeowners and customers using Kandua's platform or services.
 - Service Providers ("Pros") registered on the Kandua platform or ecosystem.
 - Employees, contractors, and job applicants.
 - Business partners, insurers, vendors, and affiliates with whom Kandua engages.
- All **Kandua personnel**, including full-time and temporary staff, contractors, and third-party operators acting on Kandua's behalf, who are required to comply with the standards and obligations outlined in this policy.

This policy does **not** apply to personal or household activities conducted by individuals in their private capacity or to information that has been **de-identified** such that the data subject cannot be re-identified.

Legal and Governance Framework

Alignment with POPIA, GDPR (if applicable), and other data protection laws

Kandua is committed to full compliance with the **Protection of Personal Information Act, No. 4 of 2013 (POPIA)**, which gives effect to the constitutional right to privacy and regulates the lawful processing of personal information. Kandua also aligns its practices with the **Promotion of Access to Information Act, No. 2 of 2000 (PAIA)**, ensuring transparency, accessibility, and accountability in its information management processes.

Where applicable, Kandua recognises and incorporates the principles of international data protection frameworks such as the **General Data Protection Regulation (GDPR)** of the European Union, particularly in relation to data subject rights, cross-border data transfers, and information security safeguards.

This policy also considers sector-specific regulatory requirements relevant to Kandua's business operations, including:

- The **Financial Advisory and Intermediary Services Act (FAIS)**;
- The **Consumer Protection Act (CPA)**;
- The **Electronic Communications and Transactions Act (ECTA)**; and
- The **Insurance Act (No. 18 of 2017)**, insofar as Kandua operates within Santam's insurance ecosystem.

Through this integrated compliance approach, Kandua ensures that all personal information is processed in a lawful, fair, and transparent manner, consistent with both local and global privacy standards.

Group Governance and Oversight

Kandua aligns its privacy governance model with the **Santam Group Privacy Policy (2021)** and broader **Santam Group Governance Framework**, ensuring that all privacy and data protection practices are consistent with the controlling company's policies, oversight structures, and compliance expectations.

In accordance with Santam's data protection principles, Kandua adopts the following governance approach:

- **Accountability** for personal information processing rests with Kandua's executive management, under oversight from the Santam Group Compliance and Governance structures.
- Kandua's privacy practices are guided by the **Kandua Group Information Officer**, and any cross-entity sharing of data or joint processing activities are conducted in alignment with Santam's **Binding Corporate Rules (BCRs)** and **Group Data Protection Standards**.
- All privacy and security controls implemented within Kandua's systems are required to meet the minimum standards prescribed by Santam's **Information Security Policies** and **Data Management Guidelines**.

Kandua commits to reporting material data incidents, compliance breaches, or regulatory notifications to Santam's Group Compliance Office, ensuring continuous alignment and transparent oversight within the Group.

Roles and Responsibilities

Information Officer

The **Information Officer (IO)** is formally appointed in terms of **Section 55 of POPIA** and **Section 51 of PAIA**, and is accountable for ensuring that Kandua complies with all legal requirements relating to personal information.

The IO's responsibilities include:

- Overseeing implementation of this Privacy Policy and related data protection frameworks.
- Acting as the primary liaison with the **Information Regulator of South Africa** and the **Santam Group Information Officer**.

- Approving data protection procedures, privacy notices, and security safeguards.
- Ensuring that privacy impact assessments (PIAs) are conducted for new systems, projects, and partnerships.
- Coordinating the investigation and reporting of security incidents and data breaches.
- Maintaining Kandua's **PAIA Manual** and ensuring its publication and periodic review.

Designated Information Officer:

Name: Vinolan S. Pillay

Position: Chief Executive Officer, Kandua

Email: info@kandua.com

Telephone: +27 10 1421 480

Deputy Information Officer

The **Deputy Information Officer (DIO)** supports the IO in managing day-to-day compliance operations, responding to data subject requests, and coordinating training and communication across departments.

Key duties include:

- Assisting in the maintenance of privacy registers and records of processing activities.
- Supporting data subjects with access, correction, or deletion requests under POPIA and PAIA.
- Managing internal data protection awareness campaigns and employee training sessions.
- Acting as the operational escalation point for privacy and information-related enquiries.

Designated Deputy Information Officer:

Name: Shannon Mackrill

Position: Head of Growth, Kandua

Email: info@kandua.com

Telephone: +27 10 1421 480

Cluster / Entity Information Officers

In line with **Santam Group Policy Section 5**, Kandua may appoint or designate **Entity Information Officers** within specific business clusters (e.g., Marketplace, Insurance, or Partner Operations) to ensure that privacy compliance is effectively implemented at operational levels.

These officers are responsible for:

- Overseeing compliance within their business unit or ecosystem.
- Ensuring operational adherence to POPIA and this Privacy Policy.
- Conducting privacy risk assessments and reporting to the IO or DIO on data-related matters.
- Monitoring adherence to Santam's Group Privacy Principles and ensuring consistency across platforms.

Employee Responsibilities and Training

All Kandua employees, contractors, and temporary staff are required to comply with this Privacy Policy, related Standard Operating Procedures (SOPs), and any additional instructions from the IO or DIO regarding the handling of personal information.

Employees are expected to:

- Treat all personal information as confidential business information.
- Use personal information only for authorised purposes.
- Immediately report any suspected data breach or unauthorised disclosure to the DIO or IO.

- Complete mandatory **Data Privacy and POPIA training** annually, as part of Kandua's compliance programme.

Kandua promotes a culture of privacy awareness through induction training, quarterly refreshers, and targeted campaigns, ensuring that staff understand their obligations and the potential risks associated with mishandling information.

Privacy Principles

Kandua is committed to processing personal information responsibly, transparently, and in alignment with the **Santam Group Privacy Principles** and **POPIA's eight conditions for lawful processing**. These principles govern how personal information is collected, used, shared, stored, and safeguarded across all Kandua ecosystems and systems.

Accountability

Kandua accepts full accountability for ensuring that personal information under its control is processed in accordance with POPIA, PAIA, and this Privacy Policy.

The **Information Officer** is ultimately responsible for overseeing compliance, supported by the **Deputy Information Officer** and **Entity Information Officers** in each business area.

Kandua maintains documented policies, procedures, and technical controls to demonstrate compliance with privacy laws and Santam Group standards. Regular assessments and internal audits are conducted to measure and evidence this compliance.

Lawful and Fair Processing

All personal information is processed **lawfully, fairly, and in a manner that does not infringe the privacy rights** of data subjects.

Kandua will only process personal information where a **legitimate basis** exists under POPIA or other applicable laws.

These lawful bases include:

- The data subject's **consent**;

- The **performance of a contract**;
- **Legal or regulatory obligations** (e.g., under FAIS, the Insurance Act, or the Companies Act);
- **Legitimate interests** pursued by Kandua or a third party; and
- **Protection of the data subject's vital interests.**

No personal information will be collected or used in a manner that is excessive, misleading, or incompatible with the stated purpose of collection.

Purpose Specification

Personal information is collected for **specific, explicitly defined, and lawful purposes** related to Kandua's business activities.

These purposes include, but are not limited to:

- Facilitating job connections between customers and verified service providers;
- Managing onboarding, verification, and vetting of service providers;
- Administering insurance and claims processes in partnership with Santam and other insurers;
- Performing contractual and legal obligations; and
- Improving customer experience and operational efficiency.

Any new or secondary purpose for which personal information is processed must be reviewed by the **Information Officer** to ensure it remains compatible with the original purpose and complies with POPIA.

Data Minimisation and Processing Limitation

Kandua collects and processes **only the minimum personal information necessary** to fulfil the stated purpose.

All processing is relevant, adequate, and not excessive.

Personal information is collected directly from the data subject wherever possible. If collected from a third party (e.g., insurers, verification providers, or regulatory

databases), Kandua ensures that the source is lawfully authorised to share such information.

Retention of personal information is limited to the period required to achieve the purpose of collection or to comply with applicable laws and contractual obligations.

Transparency and Openness

Kandua is committed to **transparent and fair information practices**, ensuring that data subjects are informed about how their information is collected, used, shared, and protected.

Kandua provides accessible and plain-language **privacy notices** explaining:

- The purpose of processing and lawful basis;
- Whether the provision of information is mandatory or voluntary;
- The consequences of not providing information;
- Any intended cross-border transfers; and
- The rights available to data subjects under POPIA and PAIA.

Privacy notices are made available on Kandua's website, within digital forms, and during onboarding or job connection processes, consistent with the **Santam Group transparency principle**.

Further Processing and Compatibility

Kandua will not process personal information for any secondary or unrelated purpose unless the new purpose is **compatible with the original purpose** or required by law.

Further processing will only occur when:

- The data subject has provided **explicit consent**;
- The processing is **legally authorised**; or

- It is required to comply with contractual or regulatory obligations (e.g., insurance claims validation, fraud detection, or compliance reporting).

All compatibility assessments are conducted in accordance with the criteria prescribed under POPIA and Santam's Group Privacy Procedures.

Data Quality and Accuracy

Kandua takes reasonable steps to ensure that all personal information is **complete, accurate, and up to date**, considering the purpose for which it is processed.

Data subjects are encouraged to verify and update their information via Kandua's platform or by contacting the **Deputy Information Officer**.

Periodic data reviews, validation checks, and quality assurance audits are conducted to maintain the integrity of information used in operational, regulatory, and reporting processes.

Security Safeguards

Kandua employs a **layered information security framework** to protect the confidentiality, integrity, and availability of personal information.

In alignment with Santam Group Information Security Policies and the controls defined in Kandua's **PAIA Manual**, these safeguards include:

- Data encryption (in transit and at rest);
- Access control and identity management;
- Network firewalls and intrusion detection;
- Continuous monitoring and incident response protocols;
- Regular internal audits and penetration testing; and
- Data retention and secure destruction policies.

All third-party processors and technology vendors are contractually required to meet equivalent security standards and immediately report any suspected or

actual data breaches.

In the event of a **Security Event**, Kandua will notify the **Information Regulator**, affected data subjects, and the **Kandua Information Officer** in accordance with POPIA Section 22 and Kandua escalation protocols.

Data Subject Participation and Access

Kandua respects and upholds the rights of all data subjects to access, correct, delete, or object to the processing of their personal information.

These rights include:

- **Access** to personal information held by Kandua (via a PAIA request or data subject request form);
- **Correction or deletion** of inaccurate, irrelevant, or excessive data;
- **Objection** to processing for direct marketing or non-essential purposes; and
- **Withdrawal of consent** at any time, subject to legal and contractual constraints.

Requests for access or amendment may be submitted to info@kandua.com or directly to the **Deputy Information Officer**, as described in Kandua's **PAIA Manual**.

Kandua will respond to all verified data subject requests in line with the prescribed timelines under POPIA and PAIA, ensuring fairness, transparency, and due process.

Categories of Personal Information

Kandua processes various categories of personal information to facilitate its platform operations, fulfil contractual and regulatory obligations, and improve customer and service provider experiences.

All data processing is carried out in accordance with **POPIA**, **PAIA**, and the **Santam Group Privacy Policy**, ensuring that only information necessary for lawful and defined purposes is collected and maintained.

Personal Information Definition

“Personal Information” refers to any information that can identify, or is capable of identifying, a natural or juristic person, directly or indirectly.

This includes, but is not limited to:

- Full name, identification number, or registration details;
- Contact information such as address, telephone number, or email address;
- Online identifiers including IP addresses, geolocation, and device information;
- Employment, education, or trade qualifications;
- Financial details such as bank account information, payment history, or credit standing;
- Demographic and profiling data (e.g., gender, occupation, service preferences); and
- Any correspondence, contracts, or records linked to a person’s relationship with Kandua.

This definition aligns with **Section 1 of POPIA** and the **Santam Group definition of Personal Information**, applying throughout Kandua’s digital and operational environments.

Special Personal Information

Certain categories of personal information are classified as **Special Personal Information** due to their sensitivity and potential risk to individual privacy. Kandua applies heightened protection and limited processing conditions for such data, in line with **Section 26 of POPIA** and **Santam Group Policy Section 8**.

Special Personal Information may include:

- **Race or ethnic origin**, only when required by law or for reporting and transformation objectives;
- **Health or disability information**, when necessary for insurance, claims, or occupational safety purposes;
- **Criminal behaviour or background**, including the alleged commission of offences or results of criminal checks performed through approved

verification providers such as HURU;

- **Biometric information**, such as ID photos or facial recognition used for verification; and
- **Religious, philosophical, or political beliefs**, only where voluntarily disclosed and relevant to regulatory or partnership compliance.

This information will only be processed when:

- Explicit **consent** has been obtained from the data subject;
- Required by law or for the **establishment, exercise, or defence of a legal right**;
- Necessary for **employment or insurance-related obligations**; or
- Authorised by the **Information Regulator** under applicable data protection laws.

Information of Children and Minors

Kandua recognises the importance of protecting the personal information of minors and does not knowingly collect or process personal information of any person **under the age of 18** without the necessary consent of a **competent person (parent or guardian)**. If Kandua becomes aware that personal information from a child has been submitted without lawful consent, the data will be deleted, or consent will be verified before any further processing occurs.

Certain use cases — such as marketing campaigns, training initiatives, or family-related service requests — will undergo an explicit **Data Protection Impact Assessment (DPIA)** to ensure compliance with POPIA's additional protections for minors.

Employee and Contractor Information

As an employer, Kandua processes personal information relating to employees, job applicants, interns, and contractors for administrative, legal, and operational purposes.

Employee and contractor information may include:

- Identification and contact details (e.g., ID number, physical address, email, phone number);
- Employment contracts, role designations, and performance records;
- Payroll, tax, and remuneration information;
- Leave, training, and disciplinary records;
- Skills, qualifications, and career development data; and
- Next of kin or emergency contact details.

This information is processed for purposes of:

- Fulfilling employment contracts and statutory requirements (e.g., BCEA, LRA, Income Tax Act);
- Workforce management and development;
- Employee benefits administration and occupational health and safety compliance; and
- Security and access control within Kandua's systems and facilities.

Employee data is stored securely and accessed only by authorised Human Resources and management personnel, in line with **Santam Group HR Privacy Principles** and **Kandua's internal HR SOPs**.

Client and Partner Information

Kandua collects and processes personal information from customers, service providers ("Pros"), partners, insurers, vendors, and other third parties to support its platform services, partnerships, and contractual relationships.

Customers (Homeowners) Information may include:

- Full name, contact details, and address;
- Service request details and project-related correspondence;

- Payment information and transaction records;
- Ratings, reviews, and communications through Kandua's platform; and
- Proof of ownership or identity, where required for insurance validation.

Service Providers (Pros) Information may include:

- Identification details (ID or passport);
- Trade certificates, qualifications, and compliance documentation;
- Bank account and payment details;
- Background verification results (Criminal Background checks, company registration, tax clearance, BBBEE affidavit, liability insurance); and
- Profile photos, job history, and customer ratings.

Partners, Vendors, and Insurers Information may include:

- Company registration and tax details;
- Contact persons, communication history, and service agreements;
- Operational and claims-related information; and
- Technical or usage data generated from integrated systems

All client and partner information is processed for legitimate business purposes — including verification, service fulfilment, compliance monitoring, and relationship management — and is subject to strict data-sharing agreements and **Operator Agreements** as defined in the **Santam Group Privacy Policy**.

Cross-Reference with PAIA Manual

In accordance with **Section 8 of Kandua's PAIA Manual**, all personal information processed by Kandua is categorised under identifiable **data subjects** (customers, service providers, employees, and partners) and **associated information types**.

Kandua maintains detailed **records of processing activities** (ROPAs), outlining:

- The purpose of processing;
- Categories of data subjects and data types;
- Recipients of personal information;
- Planned cross-border transfers; and
- Information security safeguards.

These records are available upon request to the **Information Regulator** or authorised oversight bodies, in line with POPIA and PAIA requirements.

Collection and Processing of Personal Information

Kandua collects and processes personal information in a lawful, transparent, and responsible manner, ensuring that only data necessary for clearly defined purposes is obtained and used.

All collection and processing activities are aligned with the **Protection of Personal Information Act (POPIA)**, **Promotion of Access to Information Act (PAIA)**, and the **Santam Group Privacy Policy**, and are conducted with respect for the rights and expectations of data subjects.

How Information is Collected

Kandua collects personal information from several lawful sources, including direct and indirect channels, digital interactions, and third-party integrations.

Information may be collected through the following means:

Direct Collection

- When individuals create accounts or submit details on Kandua's digital platforms
- When customers request services, submit quotes, or communicate via chat, email, or telephone.

- When service providers ("Pros") register, undergo verification, or update their professional profiles.
- During employment, recruitment, or contractor onboarding processes.

Indirect or Automated Collection

- Through the use of cookies, analytics tools, and digital identifiers that capture browsing activity, IP addresses, or location data
- Through correspondence, call recordings, or system logs maintained for training, quality assurance, and compliance purposes.

Third-Party or External Sources

- Verification providers such as **HURU**, **SAQA**, or **CIPC** for identity and qualification validation.
- Financial and insurance partners (e.g., **Santam**, **4Sure**) for claims processing, policy administration, or regulatory reporting.
- Credit bureaus, payment gateways, and fraud-prevention agencies.
- Public databases or law-enforcement agencies, where permitted by law.

All indirect and third-party collections are performed under lawful agreements or with the consent of the data subject, ensuring transparency and alignment with the **Santam Group Operator Governance Standards**.

Purpose of Collection and Processing

Kandua collects personal information to enable the effective operation of its business platform and to meet legal, regulatory, and contractual obligations.

The primary purposes include:

1. Platform Operations and Service Delivery

- Facilitating job connections between customers and verified service providers.
- Managing quotations, bookings, invoicing, and customer communication.

2. Verification and Compliance

- Conducting identity, qualification, criminal, and financial checks.
- Ensuring compliance with POPIA, PAIA, FAIS, and insurance regulations.

3. Insurance and Claims Management

- Administering insurance and claims processes in partnership with Santam, 4Sure, and related insurers.

4. Customer Experience and Marketing

- Providing customer support and responding to queries.
- Offering personalised product recommendations or promotional information, in line with consent preferences.

5. Operational, Legal, and Security Requirements

- Managing employment relationships, payroll, and performance.
- Preventing fraud, safeguarding systems, and investigating incidents.
- Maintaining records for statutory and audit purposes.

Personal information will never be used for purposes unrelated to Kandua's legitimate operations without the individual's knowledge or consent.

Lawful Bases for Processing

In accordance with **Section 11 of POPIA** and the **Santam Group Lawful Processing Framework**, Kandua relies on one or more of the following lawful bases when processing personal information:

Lawful Basis	Description and Application
Consent	Voluntary, specific, and informed consent is obtained where required (e.g., for marketing, data sharing with partners, or processing of special personal information).
Contractual Necessity	Processing is required to enter into or perform a contract with a customer, service provider, partner, or employee.
Legal Obligation	Processing is necessary to comply with legislation, regulations, or lawful requests (e.g., PAIA, FAIS, Income Tax Act, Insurance Act).

Lawful Basis	Description and Application
Legitimate Interest	Processing is necessary for Kandua's legitimate interests, such as fraud prevention, security monitoring, and service optimisation, provided such interests do not override the data subject's rights.
Public Duty / Vital Interests	Processing is required to protect a person's safety or vital interests, or for purposes in the public interest.

Data subjects may withdraw consent at any time, but withdrawal may affect Kandua's ability to deliver certain services or fulfil contractual obligations.

Processing Limitation

Kandua upholds strict **processing limitation** principles to ensure that all personal information is:

- **Adequate, relevant, and not excessive** for its intended purpose;
- Collected **directly from the data subject** wherever possible; and
- Processed only for the **duration necessary** to achieve the specified purpose.

Retention periods are determined based on:

- Statutory or regulatory requirements (e.g., tax, insurance, and employment laws);
- Contractual obligations with Santam and other partners; and
- Legitimate business needs for record-keeping or dispute resolution.

Upon expiry of the retention period, data is securely **destroyed or de-identified** in accordance with Kandua's **Information Retention and Destruction Procedure**, as referenced in its **PAIA Manual (Section 8.5.1)**

Processing of Special Categories

Kandua recognises that certain personal information requires additional protection due to its sensitivity.

In accordance with **Section 26–33 of POPIA** and **Santam Group Policy Section 8**, special categories of personal information may include:

- **Race, ethnic origin, or gender** – processed for transformation or legal reporting obligations.
- **Health or medical information** – processed when necessary for insurance claims, workplace safety, or employee benefits.
- **Biometric data** – processed for identity verification or security access controls.
- **Religious or philosophical beliefs** – processed only if voluntarily disclosed and relevant for policy or partnership compliance.
- **Criminal history** – processed for background checks during vetting, onboarding, or fraud investigations.

Such processing is undertaken **only when**:

- The data subject has provided **explicit consent**;
- Required or authorised by law;
- Necessary for establishing, exercising, or defending legal rights;
- Conducted for historical, statistical, or research purposes with safeguards; or
- Approved under the **Santam Group Binding Corporate Rules** and **Information Regulator authorisations**.

Kandua applies heightened technical and organisational measures — including restricted access, encryption, and role-based permissions — to protect special personal information and prevent unauthorised use or disclosure.

Information Disclosures

Kandua is committed to processing personal information in a transparent and accountable manner.

In line with **POPIA Section 18**, **PAIA**, and the **Santam Group Privacy Policy**, Kandua ensures that all data subjects are informed about the purpose, scope, and

conditions under which their personal information is collected, processed, or shared.

This disclosure principle extends to all business and digital channels, including Kandua's website, mobile platforms, and third-party integrations.

Privacy Notice and Transparency Requirements

Kandua provides accessible and plain-language **Privacy Notices** that explain how personal information is handled.

These notices are presented at the point of collection — for example, when users register on the Kandua platform, submit service requests, or participate in partner programs.

Each Privacy Notice sets out the following minimum disclosures:

- The **identity and contact details** of Kandua as the Responsible Party;
- The **purpose** for which personal information is being collected;
- Whether the information is **mandatory or voluntary**;
- The **consequences of withholding** the information;
- The **recipients or categories of recipients** of the information;
- Whether information will be **transferred across borders**; and
- The **data subject's rights** under POPIA and PAIA.

Kandua's Privacy Notices are reviewed and approved by the **Information Officer** and remain aligned with **Santam Group's Transparency and Disclosure Framework**, ensuring consistent standards across all entities in the group.

Mandatory Disclosures in Privacy Notices

Purpose of Processing

Kandua discloses the lawful purpose for collecting personal information in every Privacy Notice.

These purposes may include, but are not limited to:

- Delivering Kandua's platform services (job connections, quoting, invoicing, communication).
- Onboarding, verifying, and monitoring service providers.
- Managing insurance and claims processes on behalf of Santam or partners.
- Complying with regulatory obligations under POPIA, PAIA, FAIS, and the Insurance Act.
- Improving service delivery, customer experience, and business analytics.
- Marketing products or services (subject to consent and opt-out provisions).

Each collection point includes a clear statement outlining the exact purpose relevant to that transaction or engagement.

Voluntary vs Mandatory Information

Kandua specifies in its Privacy Notices which categories of personal information are **mandatory** (required by law, contract, or operational necessity) and which are **voluntary**.

Examples include:

- **Mandatory:** Identity documents, tax numbers, proof of address, or bank details (for verification or payment).
- **Voluntary:** Marketing preferences, photographs, or optional demographic details.

Where information is required for service provision or compliance (e.g., to verify a service provider or process an insurance claim), Kandua will clearly state that the provision of such information is **a condition of service**.

Consequences of Refusal

If a data subject declines to provide mandatory personal information, Kandua may be unable to:

- Complete onboarding or verification processes;

- Facilitate job connections or payments;
- Process insurance or claim transactions; or
- Provide access to specific products, partnerships, or digital tools.

The potential consequences of refusal are disclosed upfront in every applicable Privacy Notice, ensuring informed decision-making by the data subject.

Source of Information

Where personal information is **not collected directly** from the data subject, Kandua discloses the source of the information and the lawful basis for obtaining it.

Examples include:

- Background checks
- Credit and payment data from **financial institutions** or **credit bureaus**;
- Insurance and claim-related data shared by **Santam** or other partners;
- Regulatory and public records (CIPC, SARS, SAPS, etc.).

All such third-party collections are governed by written agreements and performed in accordance with **POPIA Section 12(2)** and **Santam Group Operator Governance Standards**.

Intended Recipients

Personal information may be shared with the following categories of recipients, strictly for lawful and defined purposes:

- **Santam Group** entities and subsidiaries for compliance, claims, and governance purposes.
- **Insurers, partners, and service providers** involved in delivering Kandua's platform or insurance products.
- **Verification agencies** for identity and qualification checks.
- **Credit bureaus** and **payment processors** for financial validation.

- **Regulatory authorities** and **ombudsman offices** when required by law.
- **Technology vendors and operators** providing hosting, data analytics, or security services (under Operator Agreements).

All recipients are required to comply with POPIA, Santam's Information Security Standards, and Kandua's contractual privacy clauses.

Cross-Border Transfers

Kandua may transfer or store certain categories of personal information outside South Africa using secure international cloud or hosting service providers (e.g., for data storage, backup, or analytics).

When such transfers occur, Kandua ensures that:

- The recipient country or organisation provides **an adequate level of data protection**;
- **Binding corporate rules (BCRs), standard contractual clauses (SCCs)**, or equivalent safeguards are in place; and
- The data subject has been **informed of the cross-border transfer** in the relevant Privacy Notice.

Kandua's cross-border data handling aligns with **Section 72 of POPIA** and **Santam Group's International Data Transfer Policy**, ensuring consistent standards of security and lawful processing globally

Applicable Legal Authorisations

Kandua processes and discloses personal information only in accordance with **lawful authorisations**, including:

- **POPIA** and **PAIA** requirements for transparency, access, and protection;
- **Insurance Act** and **FAIS** provisions for financial and claims management;
- **Companies Act** for statutory record keeping and reporting;
- **Income Tax Act** for financial compliance; and

- **Santam Group Privacy Policy** and internal authorisations for shared processing across the group.

Any disclosures required by law (e.g., to regulatory or law enforcement bodies) will be made only after verification of a valid legal basis or court order.

Use and Sharing of Information

Kandua recognises that personal information must be shared only where necessary, legitimate, and appropriately safeguarded.

All information sharing is conducted in strict accordance with **POPIA**, **PAIA**, and **Santam Group Privacy Governance Standards**, ensuring that any transfer of personal information — internally or externally — maintains confidentiality, integrity, and lawful purpose.

Intra-Group Information Sharing

Kandua operates as part of the **Santam Group of Companies** and may share personal information with Santam and its authorised subsidiaries, affiliates, and governance entities, where such sharing is necessary to:

- Facilitate joint operations and claims management;
- Support compliance, audit, or risk oversight functions;
- Align customer and service provider data for legitimate business or regulatory purposes; and
- Implement Santam's Group-wide information security and data protection standards.

All intra-group data sharing occurs under **Santam's Binding Corporate Rules (BCRs)**, internal **Data Sharing Protocols**, and **Group Privacy Policy**, which collectively ensure that the same level of protection applies across all entities within the group.

Kandua remains the **Responsible Party** for all personal information it collects, even when shared with Santam or other group entities, and continues to be accountable for ensuring lawful and secure processing.

Disclosure to Authorised Third Parties (Operators)

Kandua may engage approved third parties — known as **Operators** under POPIA — to process personal information on its behalf.

These Operators perform specific services that are essential to Kandua's business operations, including:

- Cloud hosting and infrastructure management;
- Customer communication platforms
- Background verification services
- Insurance administration, claims processing, and partner integrations;
- Payment processing and accounting systems; and
- Security monitoring, analytics, and IT support.

Kandua ensures that all Operators:

- Are contractually bound to process information only on Kandua's documented instructions;
- Implement **appropriate technical and organisational safeguards**; and
- Are regularly assessed through compliance reviews and audits to verify adherence to POPIA and **Santam Group Security Standards**.

Operators are expressly prohibited from using personal information for their own purposes or disclosing it to unauthorised third parties.

Operator Agreements and Due Diligence

Before appointing any third-party Operator or vendor, Kandua conducts a structured **Privacy and Information Security Due Diligence** review to assess:

- Data protection maturity and compliance with POPIA and GDPR (if applicable);
- Security certifications and access control measures;
- Breach response and incident reporting capabilities; and
- Cross-border transfer mechanisms and data storage locations.

All Operators are bound by written **Operator Agreements** that include:

- Defined roles and processing purposes;
- Confidentiality and non-disclosure obligations;
- Requirements for breach notification within defined timeframes;
- Prohibitions on unauthorised sub-processing; and
- Mandated alignment with Santam's Group Privacy and Information Security Frameworks.

These agreements are reviewed periodically by Kandua's **Information Officer** and **Legal/Compliance teams** to ensure continued compliance and operational effectiveness.

Disclosure to Competent Authorities

Kandua may disclose personal information to competent authorities, law enforcement agencies, or regulatory bodies when required to do so by law or valid legal process.

Such disclosures may occur under:

- **PAIA** (upon lawful request for access to records);
- **Court orders, subpoenas, or statutory notices**; or
- **Legal obligations** under the Insurance Act, FAIS Act, or tax legislation.

Before any disclosure is made, Kandua verifies the authenticity and scope of the request, ensures that disclosure is limited to the minimum data necessary, and maintains an auditable record of the release.

Where the disclosure involves data subjects within Santam's insurance ecosystem, the **Santam Group Legal and Compliance Office** is notified to ensure group-level governance and alignment with the **Santam Incident Escalation Protocol**.

Third-party Data Processors and Vendors

Kandua engages trusted third-party vendors and service providers to support its digital infrastructure, data analytics, and operational services.

These include, but are not limited to:

- **Technology partners** for platform hosting and product development;

- **Insurance and financial partners** for claims and coverage administration;
- **Compliance and verification vendors** for vetting and due diligence; and
- **Payment service providers** and **banks** for transaction processing and reconciliation.

Each vendor is subject to privacy risk assessment and contractual control, ensuring:

- Data processing is limited to legitimate and defined business purposes;
- Adequate data security and encryption protocols are in place;
- Information is not retained beyond the agreed retention period; and
- Immediate reporting of data incidents or unauthorised access.

Kandua and its vendors adhere to the **Santam Group Third-Party Risk Management Framework**, ensuring consistency and accountability throughout the data supply chain.

Prohibition on Sale of Personal Information

Kandua does **not sell**, rent, trade, or otherwise monetise personal information.

Any use of personal data for marketing, analytics, or product development is conducted in a **non-identifiable or aggregated form**, and only with the necessary **consent or lawful justification**.

Kandua's business model is built on trust, transparency, and compliance — and expressly prohibits the commercialisation or unauthorised exploitation of personal data, in alignment with **Santam Group Ethical Data Practices Policy** and **POPIA Section 11(1)** principles.

Cross-border Transfers

Kandua may transfer or store personal information outside the Republic of South Africa in limited circumstances, where it is necessary for lawful business operations, technology enablement, or compliance with contractual and group-level requirements.

All such transfers are conducted in accordance with **Section 72 of the Protection of Personal Information Act (POPIA)**, the **Santam Group Privacy Policy**, and applicable international data protection standards.

Kandua ensures that personal information continues to receive an equivalent level of protection, regardless of where it is processed or stored.

Conditions for International Transfers

Kandua transfers personal information across borders only when one or more of the following legal conditions are met:

1. **Adequate Protection:** The recipient country, organisation, or international framework provides an adequate level of protection for personal information, as recognised by the **Information Regulator** or **Santam Group Compliance**.
2. **Contractual Necessity:** The transfer is required for the performance of a contract with the data subject or a third party acting on their behalf (e.g., insurance claims, payment processing, or partner integrations).
3. **Data Subject Consent:** The data subject has given explicit, informed consent to the cross-border transfer.
4. **Legal or Regulatory Obligation:** The transfer is required by law, regulation, or a binding order from a competent authority.
5. **Group Compliance Framework:** The transfer occurs within the **Santam Group** under approved **Binding Corporate Rules (BCRs)** or equivalent mechanisms ensuring data protection consistency.

Kandua never transfers personal information internationally without confirming that the recipient jurisdiction, Operator, or partner applies lawful and adequate protection measures.

Safeguards and Legal Justifications

To ensure ongoing compliance and data protection, Kandua applies the following safeguards to all international transfers:

- **Contractual Safeguards:**

All Operators, partners, and cloud providers receiving personal information outside South Africa are bound by written agreements containing data

protection clauses that meet or exceed **POPIA Section 72(1)** and **Santam Group Security Standards**.

These agreements typically include **Standard Contractual Clauses (SCCs)**, **Data Processing Addenda (DPAs)**, or **Group-approved BCR commitments**.

- **Technical and Organisational Measures:**

Kandua ensures that personal information transferred across borders is encrypted, access-controlled, and subject to continuous monitoring.

Access is restricted to authorised personnel only, and all systems are designed with **privacy-by-design and privacy-by-default** principles.

- **Regulatory Oversight:**

Kandua maintains transparency with the **Information Regulator of South Africa** and the **Santam Group Compliance Office** for all material cross-border transfers, ensuring lawful oversight and traceability.

Where transfers involve joint operations with Santam, 4Sure, or other financial services partners, Kandua aligns with Santam's **Cross-Border Data Handling Policy**, which incorporates equivalent controls under **GDPR Article 46** frameworks.

Cloud Storage and Data Residency Considerations

Kandua makes use of secure, reputable cloud service providers and international hosting platforms to support its operations, including data storage, processing, and backup.

Such providers may operate in or replicate data to countries outside South Africa (e.g., the European Union, United States, or United Kingdom).

Before any cloud deployment, Kandua ensures that:

- The provider has robust **ISO 27001**, **SOC 2**, or equivalent data security certifications;
- All personal information is encrypted both **in transit** and **at rest**;
- Data centres are located in jurisdictions offering data protection standards comparable to those under **POPIA** and **GDPR**; and

- The provider agrees to maintain data sovereignty obligations and notify Kandua of any legal requests for disclosure.

Kandua remains the **Responsible Party** for all information stored in the cloud and retains control over how and where personal data is processed.

Record-keeping for Cross-border Processing

In accordance with **POPIA Regulation 4(1)(b)** and **Santam Group Information Governance Standards**, Kandua maintains a detailed **Register of Cross-Border Processing Activities**, which includes:

- Categories of personal information transferred;
- Purpose of each transfer and recipient details;
- Applicable legal basis and contractual safeguards;
- Jurisdictions or storage locations involved; and
- Retention and deletion timelines.

This register forms part of Kandua's broader **Record of Processing Activities (ROPA)** and is reviewed annually by the **Information Officer** in collaboration with **Santam Group Compliance**.

All cross-border transfers are traceable, auditable, and subject to oversight under both Kandua's **PAIA Manual** and **Santam Group Data Protection Framework**, ensuring accountability and lawful international data handling.

Security Safeguards and Controls

Kandua recognises that the protection of personal information is fundamental to maintaining trust and compliance with data protection laws.

The company applies a **layered security framework** designed to safeguard the **confidentiality, integrity, and availability** of personal information throughout its lifecycle — from collection to destruction.

All security practices are aligned with the **Santam Group Information Security Policy, POPIA, PAIA**, and relevant **international security standards** (e.g., ISO/IEC 27001).

Technical and Organisational Measures

Kandua implements a comprehensive set of technical and organisational measures ("TOMs") to prevent unauthorised access, loss, or damage to personal information.

These measures are regularly reviewed and updated based on emerging threats, risk assessments, and Santam Group directives.

Core measures include:

- **Role-based access management** ensuring only authorised personnel access specific data.
- **Multi-factor authentication (MFA)** for systems containing personal or financial data.
- **Data encryption**, both in transit and at rest.
- **Network segmentation** and continuous monitoring for suspicious activity.
- **Regular patch management and vulnerability assessments.**
- **Backup and recovery protocols** to ensure data resilience.
- **Privacy-by-design** and **privacy-by-default** integration into system development and third-party integrations.

These controls are tested periodically through **internal audits, penetration testing, and Santam Group assurance reviews.**

Encryption and Access Control

Kandua ensures that personal information is protected using industry-standard encryption and controlled system access protocols.

- **Encryption Standards:** All personal information transmitted electronically is encrypted using secure transport protocols (TLS/SSL). Data stored on servers, cloud environments, and databases is encrypted using AES-256 or equivalent standards.

- **Access Controls:** Access to personal information is granted strictly on a “least privilege” and “need-to-know” basis.
- **Authentication and Monitoring:** User accounts are protected by password policies, and activity logging. Access events are monitored for anomalies, and unauthorised attempts trigger automated alerts.

System administrators are required to follow **Santam Group Security Operations Guidelines** to manage and log privileged account activities.

Incident Management and Breach Reporting

Kandua maintains a formal **Information Security Incident Management Procedure**, aligned with **Santam Group’s Data Breach and Incident Response Framework** and **POPIA Section 22**.

If a data breach or security incident occurs:

1. It is **immediately reported** to the **Deputy Information Officer** and **Information Officer**.
2. A **containment and investigation** process is initiated within predefined response timelines.
3. All relevant **evidence, logs, and communication records** are preserved for audit and compliance.
4. The **Information Regulator** and affected data subjects are notified without undue delay, in compliance with POPIA Section 22(2).
5. A **root cause analysis** is conducted, and remedial actions are tracked to closure.

Kandua also reports all significant incidents involving shared data or systemic vulnerabilities to **Santam Group Compliance**, ensuring coordinated governance and oversight.

Third-party Security Compliance

Kandua ensures that all **Operators, vendors, and service providers** processing personal information on its behalf meet equivalent security and compliance standards.

This includes:

- Conducting **due diligence** and **security risk assessments** before onboarding any third-party Operator.
- Requiring formal **Operator Agreements** with defined security clauses, confidentiality obligations, and breach notification requirements.
- Performing **annual compliance reviews** or requesting third-party assurance certifications (e.g., ISO 27001, SOC 2, PCI DSS).
- Enforcing **Santam Group Third-Party Risk Management (TPRM)** requirements for any external processing or data sharing activity.

Failure by a vendor or partner to maintain appropriate security controls constitutes a material breach of contract and may result in suspension or termination of the engagement.

Physical and Cybersecurity Controls

Kandua maintains physical and digital safeguards to protect information assets within its facilities and technology environment:

Physical Controls:

- Restricted access to Kandua offices and data storage facilities using keycard or biometric access.
- Visitor logging, CCTV surveillance, and secure workstation policies.
- Locked storage for physical files containing personal or confidential data.

Cybersecurity Controls:

- Firewalls, intrusion detection, and endpoint protection systems.
- Network monitoring and incident response capabilities.
- Secure data transfer protocols between Kandua and its partners.
- Segregation of development, testing, and production environments.

Physical and cyber controls are routinely reviewed by **IT Operations** and audited under **Santam Group Information Security Governance Reviews**.

Employee Responsibilities and Breach Escalation

Every Kandua employee, contractor, and temporary staff member is personally responsible for protecting the information they handle.

All employees are required to:

- Adhere to Kandua's **Information Security and POPIA Awareness Training**, completed upon onboarding and refreshed annually.
- Use company systems responsibly and report suspicious activity or potential breaches immediately to the **Deputy Information Officer** at info@kandua.com
- Refrain from sharing passwords, storing data on unauthorised devices, or forwarding personal information to unapproved channels.
- Participate in regular security and phishing awareness campaigns managed by the **Compliance and Risk team**.

Escalation Pathway for Security Events:

1. **Detection:** Any employee who suspects or detects a breach reports it immediately via internal escalation channels
2. **Containment:** The IT Security and Compliance teams isolate affected systems and prevent further unauthorised access.
3. **Notification:** The IO assesses legal notification requirements to the **Information Regulator, Santam Group**, and affected data subjects.
4. **Post-Incident Review:** Findings are documented in Kandua's **Incident Register**, with lessons learned integrated into training and control updates.

This disciplined, multi-layered approach ensures that Kandua remains **resilient, compliant, and aligned** with both POPIA obligations and the **Santam Group Information Security Management System (ISMS)**.

Data Storage and Retention

Kandua manages personal information throughout its lifecycle — from collection to lawful disposal — to ensure compliance with **POPIA, PAIA, and Santam Group Data Retention Standards**. All data storage and retention activities are designed to uphold **data minimisation, purpose limitation, and security-by-design** principles.

Retention Periods

Kandua retains personal information only for as long as it is necessary to:

- Fulfil the specific purpose for which it was collected;
- Comply with legal, contractual, or regulatory obligations;
- Maintain business records required for audit or risk management; or
- Establish, exercise, or defend legal claims.

Typical retention periods may include:

Category of Record	Indicative Retention Period	Legal or Business Basis
Customer and Service Provider records (jobs, claims, communications)	Minimum of 5 years	POPIA, PAIA, Consumer Protection Act, Insurance Act
Employee and HR records	Minimum of 5 years after termination	BCEA, LRA, Income Tax Act
Financial and transaction records	Minimum of 7 years	Companies Act, SARS Regulations
Insurance and claim-related data	As per policy or contractual term with Santam	Insurance Act, FAIS
Operational correspondence, audit logs	Minimum of 2 years	POPIA, Santam Group Retention Policy
Legal and compliance documentation	Until resolution or expiry of statutory limitation	PAIA, Companies Act

Where no legal requirement applies, Kandua defines retention periods based on operational necessity and Santam's Group Retention Schedule.

Destruction and De-identification

When personal information is no longer required for the purpose it was collected, Kandua securely destroys or de-identifies the data in accordance with **POPIA Section 14(4)** and **Santam Group Information Disposal Procedures**.

- **Destruction:**

Paper records are shredded or incinerated. Electronic files are securely deleted, and backups are purged from servers or cloud repositories.

- **De-identification:**

Data that may be useful for analytics or service improvement is anonymised to remove any attributes that could identify an individual.

Destruction or de-identification processes are documented in Kandua's **Information Disposal Register** and subject to internal and Santam Group compliance audits.

All Operators and third-party processors are required to certify the destruction of data held on Kandua's behalf.

Archiving for Statistical, Research or Legal Purposes

In certain circumstances, Kandua may retain or archive de-identified information beyond the standard retention period for:

- **Statistical, research, or performance monitoring purposes;**
- **Legal or regulatory record-keeping;** or
- **Business continuity and historical analysis.**

When information is retained for these extended purposes, Kandua ensures that:

- The data is **de-identified or pseudonymised** where feasible;
- Access is restricted to authorised personnel only;
- Data is stored in secure, access-controlled environments; and
- It is **not used** for any purpose other than that for which it was originally retained.

These extended archiving practices are reviewed annually by the **Information Officer** to ensure continued necessity and compliance with **Santam Group Governance Requirements**.

Restriction of Processing after Purpose Fulfilment

Once the primary purpose for processing personal information has been achieved, Kandua enforces **processing restrictions** to ensure that data is no longer actively used or shared.

This may include:

- Moving records into restricted-access “archive” states ~~within Unity, Jotform, or Notion systems;~~
- Limiting employee or partner access to only those with lawful retention duties;
- Flagging or “locking” data that is subject to pending litigation, audit, or regulatory review; and
- Documenting the restricted status in Kandua’s **Records of Processing Activities (ROPA)**.

Data under restricted processing remains protected by Kandua’s **Information Security Controls** until it is either securely deleted or anonymised.

By managing data in this structured and disciplined manner, Kandua ensures that personal information is retained **only as long as necessary**, handled responsibly, and securely disposed of in line with **POPIA, Santam Group standards, and good governance principles**.

Direct Marketing

Kandua respects the right of every individual to control how their personal information is used for marketing purposes.

All direct marketing activities are conducted in accordance with **POPIA Section 69, Santam Group Marketing Compliance Policy, and FSCA Treating Customers Fairly (TCF)** principles.

Kandua ensures that all marketing communications are transparent, relevant, and based on valid consent or other lawful grounds, and that individuals can easily manage their preferences at any time.

Consent and Opt-in/Opt-out Requirements

Kandua only sends direct marketing communications where:

- The **data subject has provided explicit, voluntary, and informed consent** (opt-in); or
- The **data subject is an existing customer**, and the communication relates to similar products or services previously engaged (subject to a valid opt-out option).

Consent is obtained through clear consent statements embedded in Kandua's digital touchpoints, such as:

- Registration forms on the Kandua website or app;
- Quotation, job request, or service provider onboarding forms; and
- Promotional or feedback subscription prompts (e.g., email, SMS, WhatsApp).

Each communication contains a **visible and functional opt-out mechanism**, allowing recipients to withdraw consent immediately and without penalty.

Withdrawal of consent does not affect the lawfulness of marketing already sent before such withdrawal.

Communication Preferences and Records

Kandua maintains a **Marketing Preferences Register**, documenting:

- Consent received (opt-in records and timestamps);
- Communication channels authorised (email, SMS, in-app, phone, etc.);
- Opt-out requests and suppression lists; and
- Relevant source of consent (direct, indirect, or third-party referral).

This register ensures compliance with **POPIA Section 69(3)** and the **Santam Group Privacy Governance Standards**, enabling full audit-ability of consent and withdrawal history.

Customers and service providers can review or amend their communication preferences by:

- Accessing their profile settings on Kandua's digital platform;
- Contacting the **Information Officer** via info@kandua.com; or

- Clicking the “unsubscribe” or “manage preferences” link in any email or SMS communication.

Restrictions on Unsolicited Communications

Kandua strictly prohibits **unsolicited marketing communications** where:

- The recipient has not provided prior consent; or
- The message is not related to products or services legitimately associated with an existing relationship.

To prevent such violations, Kandua:

- Maintains **blacklists/suppression lists** to prevent accidental re-contact;
- Ensures that marketing partners and Operators use Kandua’s verified consent lists only; and
- Regularly audits campaign databases and partner integrations to verify compliance with **POPIA, Santam Group marketing guidelines, and FSCA Conduct Standards.**

Any Operator or third party found engaging in unsolicited communication on Kandua’s behalf will be subject to investigation, contract termination, and potential regulatory escalation.

Rights to Object to Marketing

Under **POPIA Section 69(4)**, every data subject has the right to:

- **Object at any time** to the processing of their personal information for direct marketing purposes;
- **Withdraw consent** to receive promotional or commercial communications; and
- **Request confirmation** that their details have been removed from marketing databases.

Kandua facilitates these rights through simple, accessible channels, ensuring no discrimination or adverse consequence for exercising such rights.

Upon receipt of an objection or opt-out request, Kandua immediately updates the suppression register to prevent further marketing contact.

In addition, Kandua's marketing team receives regular training on consent-driven communication practices, aligned with the **Santam Group Ethical Marketing Framework** and **Kandua's Treating Customers Fairly Policy**.

Automated Decision-making and Profiling

Kandua makes use of technology-driven processes to improve efficiency, accuracy, and fairness in its service delivery — including digital vetting, risk screening, and customer experience optimisation.

While certain functions involve automated data analysis or profiling, Kandua ensures that all such processing is conducted **lawfully, transparently, and with safeguards for individual rights**.

Automated decision-making is never used to make decisions that produce **legal effects or significant impact** on individuals without appropriate human oversight.

Conditions for Automated Decisions

Automated decision-making or profiling is applied only under the following lawful conditions:

1. **Consent:** The data subject has provided explicit consent for their personal information to be used in automated assessments (e.g., job matching, ratings, or recommendation algorithms).
2. **Contractual Necessity:** The automation is necessary to enter into or perform a contract with the data subject (e.g., automatically matching a customer with a suitable service provider).
3. **Legal Authorisation:** The processing is authorised by applicable law or regulatory framework (e.g., fraud screening or sanctions checks required under financial services regulations).

All automated systems undergo **ethical, privacy, and accuracy assessments** as part of Kandua's **Data Governance and Risk Review Process**, ensuring that decisions are objective, proportionate, and fair.

Right to Human Intervention

In compliance with **POPIA Section 71(2)** and **Santam Group Data Ethics Policy**, every individual subject to an automated decision has the right to:

- **Request an explanation** of the logic or criteria used;
- **Challenge the outcome** of an automated assessment; and
- **Request human review** of any decision that materially affects them.

Kandua ensures that such requests are handled promptly by authorised decision-makers (e.g., the relevant Operations, Risk, or Compliance teams).

All appeals are documented in Kandua's **Automated Decision Log**, maintained under the oversight of the **Information Officer**.

Transparency in Logic Used

Kandua maintains transparency around how algorithms, scoring systems, and data models influence operational decisions.

Without revealing proprietary logic or trade secrets, Kandua provides meaningful explanations regarding:

- The **data inputs** considered (e.g., job history, rating scores, verification status);
- The **purpose** of the algorithm (e.g., efficiency, fraud detection, service matching);
- The **impact** of automated processing on users; and
- The **mitigation measures** in place to prevent bias or discriminatory outcomes.

All automated systems are periodically reviewed by Kandua's **Technology and GRC functions**, in alignment with **Santam Group AI Governance Frameworks**, to ensure that outputs remain accurate, fair, and non-discriminatory.

Protection of Legitimate Interests

Kandua applies appropriate technical and organisational measures to safeguard the **legitimate interests and rights** of all individuals affected by automated processing, including:

- Implementing **bias detection and fairness testing** within algorithms;
- Ensuring that data used for profiling is **relevant, accurate, and up to date**;
- Limiting automation to purposes consistent with **Kandua's contractual and regulatory obligations**; and
- Maintaining **audit trails** and independent review mechanisms for all high-impact automated processes.

Where profiling contributes to service personalisation or business analytics, Kandua ensures that such activities are **de-identified or aggregated**, avoiding any decision that could unfairly prejudice a person's rights, access, or reputation.

All automated decision-making practices are overseen by the **Information Officer** and remain subject to **Santam Group Data Ethics and Governance Committees**, ensuring ongoing accountability, transparency, and compliance with both **POPIA Section 71** and **GDPR Article 22** principles.

Data Subject Rights

Kandua is committed to upholding the privacy rights of all individuals whose personal information it processes.

These rights are protected under the **Protection of Personal Information Act (POPIA)**, **Promotion of Access to Information Act (PAIA)**, and the **Santam Group Privacy Policy**.

Data subjects may exercise their rights at any time by submitting a written request to **info@kandua.com** or the **Information Officer** listed in Kandua's **PAIA Manual**.

Right of Access

Every individual has the right to request confirmation as to whether Kandua holds any personal information about them and, if so, to obtain:

- A record or description of that information;

- The purpose for which it is being processed; and
- The categories of recipients to whom the information has been or may be disclosed.

Requests for access must be submitted in accordance with the procedures described in **Kandua's PAIA Manual**.

Access may be refused only where permitted under PAIA (for example, where disclosure would compromise another person's rights or legal privilege).

Right to Rectification or Correction

Individuals have the right to request that Kandua **correct, complete, or update** any personal information that is inaccurate, outdated, or incomplete.

Upon receiving a valid correction request:

- Kandua will update its records promptly and confirm the change;
- All Operators or third parties who previously received the incorrect information will be notified (where applicable); and
- Proof of correction will be logged in the **Data Subject Request Register**.

This process aligns with **POPIA Section 24** and **Santam Group Data Accuracy Standards**.

Right to Erasure

A data subject may request that Kandua **delete or destroy** their personal information where:

- The information is no longer necessary for the purpose it was collected;
- The data subject withdraws consent and no other lawful basis exists for processing;
- The information was unlawfully obtained or processed; or
- Erasure is required to comply with a legal obligation.

Kandua will assess such requests against its **legal retention and business obligations** (e.g., insurance claims, audit records, or statutory record-keeping).

Where deletion is not immediately possible, Kandua will apply **processing restriction** until lawful destruction can occur.

All erasure actions are documented in Kandua's **Information Disposal Register**, as required under **Santam Group Records Retention Policy**.

Right to Restrict Processing

Data subjects may request that Kandua temporarily **suspend or limit the processing** of their personal information under specific circumstances, such as:

- Contesting the accuracy of data (pending verification);
- Objecting to processing under POPIA Section 11(3);
- Where processing is unlawful but the data subject prefers restriction to deletion; or
- When Kandua no longer requires the data but the subject needs it for legal claims.

Restricted data is "frozen" in a secure environment — inaccessible to most users and excluded from any further processing — until the restriction is lifted or resolved.

Right to Object

Under **POPIA Section 11(3)** and **Section 69(4)**, individuals have the right to **object to the processing** of their personal information, particularly for:

- Direct marketing communications;
- Profiling or automated decision-making that materially affects them; or
- Processing carried out on the basis of legitimate interest.

Kandua provides simple mechanisms to exercise this right — such as **unsubscribe links, email notifications**, or a direct written objection to the **Information Officer**.

Upon receiving an objection, Kandua will cease processing for the specified purpose and confirm the action to the requester in writing.

Right to Data Portability

Where technically feasible and applicable, individuals have the right to **request a copy of their personal information** in a structured, commonly used, and machine-readable format.

This right applies where:

- The data subject provided the information directly to Kandua;
- Processing is based on consent or contractual necessity; and
- The data is processed through automated means.

Kandua will facilitate the secure transfer of such data either to the requester or to another controller, provided that doing so does not infringe the rights of third parties or breach confidentiality obligations.

This right is recognised under **Santam Group Data Portability and Information Sharing Principles**, aligned with **POPIA Section 23** and **GDPR Article 20** equivalents.

Right to Lodge Complaints

Data subjects who believe that Kandua has infringed their privacy rights may **lodge a complaint** through one of the following channels:

Internal Escalation:

Submit a complaint to Kandua's **Information Officer** at:

 info@kandua.com

 Attn: Information Officer, Kandua (Pty) Ltd, Cape Town, South Africa

Kandua investigates all complaints promptly and transparently, in line with **Santam Group Complaints Management Policy** and **Kandua's Escalation and Risk Management Framework**.

Regulatory Escalation:

If the matter remains unresolved, the data subject may contact:

The Information Regulator (South Africa)

JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

 complaints.IR@justice.gov.za

Kandua fully cooperates with the Information Regulator and Santam Group Compliance on all regulatory investigations and undertakes to implement any remedial action required.

Procedure for Access Requests

Kandua facilitates lawful and transparent access to personal information in accordance with the **Protection of Personal Information Act (POPIA)** and the **Promotion of Access to Information Act (PAIA)**.

The purpose of this procedure is to ensure that data subjects and authorised third parties can obtain access to personal information **efficiently, securely, and within the statutory timelines**, while protecting the rights and privacy of all parties.

All requests for access to personal information held by Kandua must follow the procedure below and comply with the formal requirements of **Section 53 of PAIA**.

PAIA Compliance and Access Request Process

Kandua has established an internal **Access to Information Process** governed by its **PAIA Manual** (available on the Kandua website).

The key steps are:

1. Request Submission:

The requester must complete the prescribed **PAIA Form C** or submit a written request containing sufficient detail to identify the record(s) sought, the requester's contact details, and the right being exercised.

2. Acknowledgment of Receipt:

Kandua's **Information Officer (IO)** or **Deputy Information Officer (DIO)** will acknowledge receipt of the request and confirm any additional documentation required for verification.

3. Assessment and Processing:

- The IO/DIO verifies whether Kandua holds the requested record.

- The IO determines whether any grounds for refusal apply under **Sections 62–70 of PAIA** (e.g., third-party confidentiality, commercial privilege, or safety concerns).
- If the record is eligible for release, arrangements are made for secure inspection, reproduction, or electronic delivery.

4. **Decision Notification:**

The requester will receive a written decision within the statutory timeframe, outlining whether the request is granted (in full or partially) or refused, with reasons provided where applicable.

Verification and Response Timelines

To ensure confidentiality and lawful disclosure, Kandua verifies the **identity and authority** of all requesters before releasing any information.

Verification may include presentation of:

- Valid identification (e.g., ID or passport);
- Proof of authorisation where acting on behalf of another person or entity; or
- A certified power of attorney or resolution for legal representatives or corporate entities.

Response Timelines:

- Kandua will respond to access requests **within 30 calendar days** of receipt, as required by **Section 56(1) of PAIA**.
- In complex cases requiring extensive searches or third-party consultation, the IO may extend the timeframe by **a further 30 days**, in which case the requester will be notified in writing.

All requests and outcomes are recorded in Kandua's **Access Request Register** for audit and compliance tracking, under oversight of **Santam Group Governance**.

Request Forms and Channels

Requests may be submitted using one of the following channels:

- **Email:** info@kandua.com

- **Post:** Information Officer, Kandua (Pty) Ltd, (address listed in PAIA Manual)
- **In-person:** By appointment at Kandua's registered office (address listed in PAIA Manual)

Required Form:

- **Form C** (Prescribed under PAIA Regulation 10) must be used for all access to personal information requests.
- The form should include:
 - Full name and contact details of the requester;
 - Description of the record requested;
 - Preferred method of access (inspection, copy, or digital format); and
 - Applicable supporting documentation (e.g., ID, authorisation letter).

Completed forms are processed by the **Information Officer** in accordance with the procedures outlined in **Kandua's PAIA Manual Section 6** and **Santam Group Access Request Protocol**.

Fees and Exceptions

Fees for access to records are determined in accordance with the **PAIA Fee Schedule** (Government Gazette Notice 187, 15 February 2002):

- **Request Fee:** A nominal fee (as prescribed) may apply to initiate a request, except where the requester is seeking access to their own personal information.
- **Reproduction Fee:** Additional costs may apply for photocopying, printing, or digital reproduction of records.
- **Deposit:** For large or complex requests, a deposit of up to one-third of the estimated cost may be required before processing begins.

Kandua may **waive or reduce fees** for personal information requests where reasonable grounds exist (e.g., hardship, data subject verification, or Santam Group governance instruction).

Grounds for Refusal:

Access may be lawfully refused under PAIA where disclosure would:

- Unreasonably disclose third-party personal information;
- Endanger the life or physical safety of an individual;
- Reveal confidential commercial information of a third party;
- Compromise ongoing investigations, legal privilege, or trade secrets.

All refusals are documented and justified in writing, and requesters are informed of their **right to appeal** or lodge a complaint with the **Information Regulator**.

Complaints and Enquiries

Kandua values transparency and accountability in its handling of personal information.

All complaints and enquiries relating to privacy, data protection, or information access are managed through a structured process that ensures **fair resolution, timely response, and regulatory compliance**.

The procedure below outlines how data subjects may raise privacy-related concerns, and the channels through which these may be resolved internally or escalated externally.

Internal Complaints Handling Procedure

Kandua encourages all data subjects to first raise any privacy, information security, or access-related concerns directly with the company for prompt resolution.

Step 1 – Submission of Complaint:

Complaints may be submitted via any of the following channels:

- **Email:** info@kandua.com
- **Post:** Information Officer, Kandua (Pty) Ltd, (address listed in PAIA Manual)
- **In-person:** By appointment at Kandua's registered office (address listed in PAIA Manual)
- Through Kandua's contact form or written correspondence addressed to the **Information Officer (IO)** or **Deputy Information Officer (DIO)**.

Each complaint must include:

- The complainant's full name and contact details;
- A description of the privacy concern or data protection issue;
- The date and nature of the incident (if applicable); and
- Any supporting documentation or correspondence relevant to the matter.

Step 2 – Acknowledgement and Logging:

- The IO/DIO will acknowledge receipt of the complaint within **5 business days**.
- The matter is logged in Kandua's **Privacy Incident and Complaints Register**, tracked under the **GRC Division** and subject to **Santam Group oversight**.

Step 3 – Investigation and Resolution:

- The IO or an appointed compliance representative investigates the complaint objectively and thoroughly.
- If the complaint relates to an Operator, partner, or Santam-affiliated entity, the matter will be coordinated jointly under the **Group Governance Framework**.
- A written response, detailing findings and proposed corrective actions (if applicable), will be provided within **20 business days** of acknowledgement.

Step 4 – Closure and Reporting:

- Once resolved, the outcome is documented in the internal register, and systemic lessons are escalated to the **Risk & Compliance Committee** for process improvement.
- If the data subject is dissatisfied with the outcome, they may escalate the matter externally to the **Information Regulator**.

External Escalation

If a data subject believes that Kandua has contravened POPIA or mishandled personal information, and is unsatisfied with Kandua's internal resolution, they may lodge a formal complaint with the **Information Regulator (South Africa)**.

Information Regulator (South Africa)

JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

 **P.O. Box 31533, Braamfontein, Johannesburg, 2017**

 **complaints.IR@justice.gov.za**

 **www.justice.gov.za/inforeg**

The complaint must be submitted in the prescribed format (Form 5 under the POPIA Regulations) and include relevant details of the alleged non-compliance.

The Information Regulator will acknowledge receipt, investigate the matter, and may take enforcement or remedial action as appropriate.

Kandua fully cooperates with the Regulator and with **Santam Group Compliance** in any investigation or inquiry, ensuring alignment with corporate governance standards and regulatory expectations.

Dispute Resolution Process

Where a complaint results in a dispute that cannot be resolved informally, Kandua follows a structured **Dispute Resolution Process**, consistent with the **Santam Group Complaints Management Framework** and **FSCA Treating Customers Fairly (TCF)** outcomes.

The process includes:

1. **Formal Mediation:** The IO engages relevant business units or external partners (e.g., Santam, 4Sure, or a data Operator) to mediate and attempt a mutual resolution.
2. **Independent Review:** If the matter remains unresolved, an internal review may be conducted by Kandua's **Risk and Compliance Committee**, ensuring objectivity and oversight.
3. **Regulatory Escalation:** Where mediation fails, or where legal implications exist, the matter may be referred to the **Information Regulator, Ombudsman, or court of competent jurisdiction** for adjudication.

Kandua ensures that all complainants are treated **fairly, respectfully, and without prejudice**, and that every complaint contributes to continuous improvement of its **data protection and governance frameworks**.

Information Officer Contact Details

In accordance with the **Protection of Personal Information Act (POPIA)** and the **Promotion of Access to Information Act (PAIA)**, Kandua has appointed an **Information Officer** and **Deputy Information Officer(s)** to oversee data protection compliance, manage information access requests, and liaise with the **Information Regulator of South Africa**.

All privacy-related queries, complaints, or access requests should be directed to the officers listed below.

Information Officer

Vinolan S Pillay, CEO, Kandua

Email: info@kandua.com

Telephone: +27 10 1421 480

Responsibilities:

- Overall accountability for POPIA and PAIA compliance;
- Oversight of policy implementation, access request handling, and breach notification;
- Liaison with the **Information Regulator** and **Santam Group Compliance**;
- Approval of data protection policies, training, and internal awareness campaigns; and
- Annual submission of compliance reports and PAIA Manual updates.

Deputy Information Officer

Shannon Mackrill, Head of Growth, Kandua

Email: info@kandua.com

Telephone: +27 10 1421 480

Responsibilities:

- Day-to-day administration of access requests and complaints;
- Managing data subject request registers and breach incident reporting;
- Coordinating with IT and Legal teams on data protection controls; and
- Supporting Santam Group governance reviews and audit readiness.

Physical and Postal Address

Kandua Head Office:

Kandua
9 Somerset Rd
Green Point
Cape Town
8001

Business Address

Telephone and Email Contact

Telephone: +27 10 142 1480

Email: info@kandua.com

Link to Online PAIA Manual

Kandua's full **Promotion of Access to Information (PAIA) Manual** — including detailed procedures for submitting access requests, the applicable fees, and the list of record categories — is available on the company's website:

<To be provided once live>

This manual forms part of Kandua's broader **Governance, Risk & Compliance (GRC) Framework**, approved by the **Information Officer** and maintained in alignment with **Santam Group Policy Governance Standards**.

Cookies and Digital Tracking

Kandua’s digital platforms — including its website, mobile applications, and partner integrations — use cookies and similar technologies to provide users with a secure, consistent, and personalised experience.

All such technologies are used in compliance with **POPIA**, **PAIA**, and the **Santam Group Digital Privacy and Data Analytics Standards**, ensuring that only data necessary for functionality, analytics, and service optimisation is collected.

Use of Cookies and Similar Technologies

A “cookie” is a small data file stored on a user’s browser or device to help websites function effectively, remember preferences, and enhance usability.

Kandua uses cookies and comparable technologies such as **web beacons**, **pixels**, **device identifiers**, and **local storage** to:

- Enable secure login sessions and maintain user authentication;
- Remember user preferences, settings, and saved jobs;
- Track service performance and troubleshoot technical issues;
- Measure engagement and improve the usability of Kandua’s digital platforms; and
- Support integration with trusted partners (e.g., analytics or communication platforms).

Cookies are not used to collect sensitive personal information such as ID numbers, financial data, or passwords.

Purpose

Kandua categorises cookies and tracking technologies based on their **purpose**:

Category	Purpose	Examples
Strictly Necessary Cookies	Essential for platform operation and security (e.g., login sessions, CSRF tokens).	Session ID cookies, authentication tokens.
Functional Cookies	Enhance functionality and remember user preferences	“Remember me” or preference cookies.

Category	Purpose	Examples
	(e.g., language, region, saved data).	
Analytics and Performance Cookies	Help Kandua and Santam Group measure traffic, detect issues, and analyse usage trends.	Google Analytics, Hotjar, or internal analytics tools.
Personalisation and Marketing Cookies	Used (only with consent) to tailor communications, advertising, or promotions to user interests.	Meta Pixel, Google Ads remarketing tags.

These cookies enable Kandua to continuously improve the user experience and service delivery, while respecting **data minimisation** and **lawful processing** principles under POPIA.

User Control and Opt-out Options

Kandua provides users with meaningful control over their cookie and tracking preferences.

Users can:

- **Manage or delete cookies** via their browser settings (most browsers allow users to refuse or delete cookies under "Privacy" or "Security" settings);
- **Adjust cookie preferences** on Kandua's website through a visible **Cookie Consent Banner**, which allows opting in or out of non-essential cookies;
- **Withdraw consent** for analytics or marketing cookies at any time without affecting access to essential site functions; and
- Use **browser-based opt-out tools** (e.g., Google Analytics Opt-Out Add-On) to prevent data collection for analytical purposes.

Declining cookies may limit certain functionality or personalised features, but essential services will remain accessible.

Kandua does **not** use cookies for unlawful tracking or to sell personal data. All cookies and tracking tools are reviewed annually as part of Kandua's **Privacy**

Impact Assessments (PIAs) and Santam Group Data Analytics Compliance Reviews.

Policy Implementation and Enforcement

Kandua enforces this Privacy Policy through an integrated framework of **governance controls, compliance monitoring, staff training, and periodic review**, ensuring full alignment with **POPIA, PAIA, and Santam Group oversight requirements**.

All employees, contractors, and partners are responsible for adhering to the standards and controls described in this policy.

Compliance Monitoring and Reporting

Kandua's **Governance, Risk & Compliance (GRC)** function, under the leadership of the **Information Officer**, monitors and reports on adherence to this policy through:

- Routine **privacy compliance reviews** and **data protection audits**;
- Continuous monitoring of access requests, breach logs, and data subject complaints;
- Quarterly **compliance status reports** submitted to the **Santam Group Compliance Office** and **Kandua Executive Committee**; and
- Integration of privacy metrics into Kandua's **Risk Register** and **GRC dashboard** (tracking risks, issues, and mitigation progress).

Findings from these reviews inform improvement actions, training updates, and, where necessary, amendments to this policy or related procedures.

Staff Training and Awareness

All Kandua employees, contractors, and temporary staff receive **mandatory privacy and data protection training** as part of the onboarding process and through annual refresher programmes.

The training covers:

- POPIA principles and data subject rights;
- Internal data handling and access protocols;
- Incident detection and breach escalation;
- Responsible use of digital tools (and
- Kandua's alignment with **Santam Group Information Security Standards**.

Departmental heads and line managers are responsible for embedding data protection awareness into day-to-day operations, ensuring that privacy principles are consistently applied across all business functions.

Disciplinary Action for Non-compliance

Non-compliance with this Privacy Policy, or with any applicable data protection law, constitutes a **serious breach of Kandua's Code of Conduct** and may lead to disciplinary action.

Depending on the nature and severity of the breach, actions may include:

- Formal warnings;
- Suspension or termination of employment or contracts;
- Removal of system access privileges; and
- Referral to law enforcement or regulatory authorities where criminal or gross misconduct is involved.

Third-party partners or Operators found in violation of contractual data protection obligations may face contract termination, financial penalties, and formal reporting to **Santam Group** and the **Information Regulator**.

All disciplinary measures are handled in accordance with Kandua's **HR Disciplinary Procedure** and **Santam Group Ethics and Compliance Framework**.

Annual Review and Updates

This Privacy Policy is reviewed **annually**, or sooner if:

- New legal, regulatory, or Santam Group requirements arise;

- Operational or technological changes materially affect data processing activities; or
- Post-incident reviews identify gaps or improvement opportunities.

The **Information Officer**, in coordination with **Santam Group Compliance** and **Kandua's Executive Team**, oversees each review cycle to ensure ongoing relevance and compliance.

Each review is documented in Kandua's **Policy Register**, with version tracking and approval records maintained in Notion under the GRC directory.

Record of Amendments

Kandua maintains a **Policy Amendment Log** to record every change made to this policy, ensuring transparency and version control.

Each entry includes:

- **Version number** and **effective date**;
- **Description of the amendment** (e.g., policy updates, scope changes, inclusion of new sections);
- **Author and approver** (Information Officer and Executive Sponsor); and
- **Link to approval record** in Kandua's GRC repository or Notion Policy Register.

Version	Effective Date	Amendment Summary	Prepared By	Approved By
1.0	14 Oct 2025	Initial draft aligned with Santam Group Privacy Policy (2021)	C. Dreyer (Admin Officer)	V. Pillay (CEO)

Definitions and Interpretation

For the purposes of this Privacy Policy, the following terms shall bear the meanings assigned to them below.

Where any term is not defined herein, its meaning shall be interpreted in accordance with the **Protection of Personal Information Act, 4 of 2013 ("POPIA")**, the **Promotion of Access to Information Act, 2 of 2000 ("PAIA")**, and other applicable South African legislation.

Unless inconsistent with the context, words importing:

- The singular shall include the plural and vice versa;
- Any gender shall include all genders; and
- Natural persons shall include juristic persons, and vice versa.

Core Definitions

Term	Definition
"Data Subject"	The natural or juristic person to whom personal information relates. This includes Kandua customers, service providers ("Pros"), employees, partners, vendors, and any individual whose data is processed by Kandua.
"Personal Information"	Information relating to an identifiable, living natural person or existing juristic person, as defined in Section 1 of POPIA . This includes, but is not limited to, names, identification numbers, contact details, financial and employment information, online identifiers, and correspondence.
"Special Personal Information"	Information regarded as sensitive under Section 26 of POPIA , including race, ethnic origin, health, biometric data, religious or philosophical beliefs, and criminal behaviour.
"Responsible Party"	A public or private body or any other person that determines the purpose of and means for processing personal information. For purposes of this policy, Kandua (Pty) Ltd acts as the Responsible Party for all information collected through its platforms and business operations.
"Operator"	A person or organisation that processes personal information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that Responsible Party (e.g., IT providers, verification agencies, or cloud service partners).

Term	Definition
"Processing"	Any operation or activity concerning personal information, including collection, receipt, recording, organisation, storage, updating, retrieval, consultation, use, dissemination, merging, linking, restriction, erasure, or destruction of information.
"Consent"	Any voluntary, specific, and informed expression of will by which a data subject agrees to the processing of their personal information, as defined in Section 1 of POPIA . Consent may be given in writing, electronically, or through a clear affirmative action.
"Information Officer"	The individual designated in terms of Section 55 of POPIA and Section 17 of PAIA as responsible for ensuring compliance with both Acts, managing access requests, and acting as the point of contact with the Information Regulator. For Kandua, this is the appointed GRC representative listed in Section 18 of this Policy.
"Deputy Information Officer"	A person authorised by the Information Officer to assist with compliance and administration of PAIA/POPIA obligations. For Kandua, this includes the operational GRC delegate(s) responsible for access requests, breach management, and training coordination.
"Information Regulator"	The statutory authority established under Chapter 5 of POPIA to monitor and enforce compliance with data protection legislation in South Africa.
"Personal Data Breach"	Any unauthorised access to, disclosure of, loss of, damage to, or destruction of personal information, whether accidental or unlawful, which compromises the security or confidentiality of such data.
"Third Party"	Any person or entity other than the data subject, Responsible Party, Operator, or any person under the direct authority of the Responsible Party or Operator.
"Santam Group"	The controlling company and its subsidiaries with which Kandua (Pty) Ltd is affiliated, forming part of the broader corporate governance and compliance oversight framework governing this policy.
"Unity Platform"	Kandua's proprietary workflow and data management system used to support job management, partner integrations, and data processing functions across its ecosystems.

Term	Definition
"Marketplace", "Insurance", "Partner", and "Pro Ecosystems"	The operational environments within which Kandua conducts business — facilitating job connections, insurance claims, partnership projects, and service provider management — collectively forming the Kandua Ecosystem.
"POPIA"	The Protection of Personal Information Act, 4 of 2013 , which promotes the protection of personal information processed by public and private bodies and establishes the rights of data subjects.
"PAIA"	The Promotion of Access to Information Act, 2 of 2000 , which provides for access to records held by public and private bodies, subject to justifiable limitations.
"GDPR"	The General Data Protection Regulation (EU) 2016/679 , referenced for consistency with international data transfer and governance standards under the Santam Group framework.

Reference to Applicable Legislation

This Privacy Policy shall be interpreted and applied in accordance with the following laws and frameworks, as amended or replaced from time to time:

1. **Protection of Personal Information Act, 4 of 2013 (POPIA)**
2. **Promotion of Access to Information Act, 2 of 2000 (PAIA)**
3. **Electronic Communications and Transactions Act, 25 of 2002 (ECTA)**
4. **Consumer Protection Act, 68 of 2008 (CPA)**
5. **Companies Act, 71 of 2008**
6. **Basic Conditions of Employment Act, 75 of 1997 (BCEA)**
7. **Insurance Act, 18 of 2017** and **Financial Advisory and Intermediary Services Act (FAIS), 37 of 2002**
8. **Santam Group Privacy Policy (2021)** and associated governance frameworks
9. **Kandua PAIA Manual (2025)** and related internal compliance procedures

These laws collectively provide the **legal, ethical, and operational foundation** for Kandua's data protection and privacy governance framework.
