DATA PROTECTION POLICY

Data Protection Policy

1 Introduction

JULICA is the data controller and processor of the information provided for registration, application, training, and certification purposes, as well as support services.

As declared in our data protection policy, we are dedicated to and responsible for processing the information of our employees, customers, stakeholders, and other interested parties with full caution and confidentiality. This policy describes how we collect, store, handle and secure our data.

The rules outlined in this document any form of data, be them stored electronically, on paper, or on any other storage device.

2 Privacy Elements

As part of our operations, we gather and process information or data that can make individuals identifiable, including, but not limited to, full name, phone number, account credentials, and home address.

The use of personal data by JULICA is governed by the Data Protection Act of Kenya, European General Data Protection Regulation (EU-GDPR), and other national privacy legislation that offer the same level of data protection as the GDPR.

We are committed to process all personal data under our control in accordance with data protection principles.

The data we process data will be:

- Processed in a lawful, fair, and transparent manner
- Collected only for specific, explicit, and limited purposes (purpose limitation)
- Adequate, relevant, and not excessive (data minimization)
- Accurate and kept up-to-date, where necessary
- Kept for no longer than necessary (retention)
- Handled with appropriate security and confidentiality

3 Roles and Responsibilities

All JULICA employees and collaborators are responsible for ensuring that the collection, storage, handling, and protection of data is done appropriately. The contact details of our Data Protection Officer are:

Person: Data Protection Officer

Email: Christina Wanjiku wood
Phone: +254795289184

The following are the responsibilities of specific people or departments:

3.1 Data Protection Officer

- Inform and advise the controller or processor and their employees of their obligations under data protection laws
- Act as a contact point for requests from individuals regarding the processing of their personal data and the exercise of their rights
- Oversee and implement data protection strategies
- Conduct regular assessments and audits to ensure GDPR compliance

3.2. Information Security Manager

- Oversee and improve cybersecurity awareness programs and risk management regularly
- Collaborate with the Security Committee in leading the design, implementation, operation, and maintenance of the information security management system.
- Ensure periodic testing are conducted to evaluate the security posture of information security
- Lead the design and operation of related compliance monitoring and improvement activities to ensure compliance both with internal security policies and applicable laws and regulations
- Develop and manage controls to ensure compliance with the requirements of various security laws, standards, and regulations

3.3. IT Systems Manager

- Strictly comply with all JULICA CA policies related to non-disclosure, non-competition, and the confidentiality of information
- Constantly stay up to date on various web technologies and tools
- Perform networking systems hardware and software upgrades and install security patches, as needed
- Check and monitor the general health of networks and networking devices
- Perform daily system monitoring, verify the integrity and availability of all hardware, server resources, systems, and IT processes, review system and application logs, and verify completion of scheduled jobs such as backups
- Implement, configure, and maintain computer networks, software, and digital security

3.4. Compliance Department

- Ensure that access to the personal data of Certification holders, Trainers, Examiners, Examinees, and Invigilators will not be shared with or provided to unauthorized parties
- Additional documents and data provided by applicants are being stored appropriately and centralized to ensure the confidentiality, integrity, availability of the data

3.5. Business Development Department

Ensure that access to JULICA Authorized users and Agents' personal data:

- Is restricted to authorized personnel only
- Will not be shared with or provided to unauthorized parties

3.6. System Administrator

Ensure that access to the personal data of members registered on the JULICA Website:

- Is restricted to authorized personnel only
- Will not be shared with or provided to unauthorized parties

4 General Guidelines

- Personal data of stakeholders shall be restricted only to employees who need it to complete their job in line with their job responsibilities.
- Informally sharing data is prohibited. When access to confidential information is needed, employees shall request it from their immediate superior.
- All JULICA CA employees shall undergo comprehensive training to help them understand their responsibilities when handling personal data.
- Data in the process by employees shall be kept secure and stored following the data storage guidelines presented in the chapter below.
- In particular, account credentials and passwords shall be kept in encrypted storage with restricted access.
- Personal data shall not be disclosed or communicated to unauthorized people, either within the company or externally.
- When unsure about any aspect of data protection, employees shall request assistance from their immediate superior or the Data Protection Officer.

5 Data Storage

These rules describe the storage and the process of safely storing data. Data is stored electronically shall be limited to authorized personnel only. The guideline also applies to electronically stored data printed out for specific reasons.

- Employees with access to electronic files shall ensure confidentiality.

Data shall be protected from unauthorized access, accidental deletion, and malicious hacking attempts.

- Data shall be protected with strong passwords that are changed regularly and never shared between employees.
- Data shall not be stored on removable media (like a CD or DVD). If necessary for job purposes, removable media shall be kept locked and secure.
- Data shall only be stored on designated servers at JULICA premises and shall only be uploaded onto approved cloud computing services.
- Servers containing personal data shall be sited in a secure location where access is restricted to authorized personnel only. The site must be monitored and access-controlled.
- Data shall be backed up daily. Backups shall be tested regularly, in line with the company's standard backup procedures.
- Data shall never be saved directly to laptops or other mobile devices (e.g., tablets or smartphones).
- All servers and computers containing data shall be protected by approved security software and a firewall.
- All data entering JULICA systems and website are stored as unique and measures to prevent privilege escalation are taken.
- All data entering into the database of the JULICA website are protected with certificates that ensure encrypted communication when receiving and sending information.

6 Data Usage

- All data collected by JULICA CA are strictly for JULICA-related services. They are used to provide complete responses or services. No other non-JULICA related service will be offered from the data collected.
- When working with personal data, employees shall ensure their computer screens are always locked when left unattended.
- Data shall be encrypted before being transferred electronically.
- Employees shall not save copies of personal data to their computers. Always access and update the central copy of any data.

7 Data Accuracy and Action

To exercise data protection, JULICA CA takes reasonable steps and is committed to:

- Restrict and monitor access to sensitive data
- Establish effective data collection procedures
- Provide employees with online privacy and security training
- Build secure networks to protect online data from cyberattacks
- Establish clear procedures for reporting privacy breaches or data misuse

- Include contract clauses or communicate statements on how we handle data
- Update the data continuously
- Ensure that marketing databases are checked against industry suppression files
- Install tracking logs to monitor employees' activities ensuring data is not being misused
- Install firewall and protection software that prevents employees from sharing and distributing data from JULICA CA devices externally by means of detecting large amounts of data being transferred via email or external drives
- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization, etc.)

8 Subject Access Requests

All individuals and organizations who are subject of personal and other data held by JULICA are entitled to:

- Ask what information JULICA holds about them and why
- Ask how to gain access to it
- Be informed on how to keep it up to date
- Be informed on how the company meets its data protection obligations

Our clients can request such information directly through a subject access request made via email or through the digital form available here. We will always verify the identity of anyone making a subject access request before handing over any information. Confirmation will be asked from the data subject using the email data subject used to register an account at JULICA. We aim to respond to the request within 14 days.

8.1 Data Modification

Our clients can request data modification or correction via email or through the digital form available. JULICA will verify the identity of anyone making a request before modifying or correcting any information.

8.2 Data Erasure

The data subject will be provided with all necessary information before erasure. Before proceeding with the erasure, the data subject will receive a statement from our Data Protection Officer explaining the outcome of the data being deleted. Erasure of data can be requested at any time.

9 Children

Our website is not intended for children or persons younger than 18. JULICA does not knowingly collect personally identifiable information (PII) of persons under the age of 18. We strive to comply with the provisions of The Data protection Act of Kenya and the European Union General Data Protection Regulation (EU GDPR). If you are a parent or custodian of a child or person under 18 years old and you believe that they have provided us with information about themselves, please contact us

10 Disclosing data

In certain circumstances, when required, JULICA can disclose data to law enforcement agencies without the consent of the data subject. However, the data controller will ensure the request is lawful, seeking assistance from the board and from the company's legal advisors, where necessary.

11 Privacy Statement.

We have a privacy statement available on our website. It presents the type information we collect, the purpose of collection and use, third-party processors involved, and how we protect customers' data. The privacy statement is available at https://tendaworld.com/policies/privacy/