

JULICA PRIVACY POLICY

Effective

Date:

27

March

2026

Version: 1.0

1. INTRODUCTION

JuliCA, operated by TendaWorld Limited, is committed to protecting the privacy and security of personal data processed in connection with its certification and trust services.

JuliCA is the data controller and processor of information provided for registration, certificate applications, training, certification and support services. This Privacy Policy sets out how JuliCA collects, uses, stores, handles, protects and discloses personal data.

This Policy applies to personal data processed by JuliCA in electronic form, in physical records and in any other form. JuliCA processes personal data in accordance with the Data Protection Act, 2019 of Kenya, the European Union General Data Protection Regulation (EU GDPR) where applicable, and other applicable data protection and privacy legislation.

2. PERSONAL DATA COLLECTED

JuliCA may collect and process personal data necessary for the provision and administration of its services, including:

- full name;
- telephone number;
- email address;
- physical or postal address;
- account credentials;
- identification and verification information;
- information contained in certificate applications;
- documents submitted in support of certificate applications;
- information relating to authorised representatives and certificate requesters;
- certificate and certificate lifecycle information;
- transaction records;
- technical and system information;
- audit and security logs; and
- other information necessary for the provision and administration of JuliCA services.

The nature and extent of personal data collected will depend on the particular service or interaction with JuliCA.

3. SOURCES OF PERSONAL DATA

JuliCA may obtain personal data:

- (a) directly from applicants, subscribers, customers and other individuals;
- (b) from authorised representatives acting on behalf of organisations;
- (c) from documents and information submitted in connection with certificate applications;
- (d) from trusted third-party sources used for identification and authentication;
- (e) from JuliCA systems and applications through the use of its services; and
- (f) from other lawful sources where necessary for the provision, administration or security of JuliCA services.

Where information obtained from a trusted third-party source is used for identification and authentication, JuliCA confirms the information with the applicant before using it.

4. PURPOSE OF PROCESSING

JuliCA processes personal data for purposes connected with its certification and trust services, including:

- receiving and processing certificate applications;
- identifying and authenticating applicants;
- verifying information submitted in certificate applications;
- issuing, managing, renewing, suspending and revoking certificates;
- administering subscriber accounts;

- providing customer and technical support;
- maintaining certificate and transaction records;
- maintaining security and audit records;
- detecting and investigating suspicious or fraudulent certificate requests;
- protecting the security and integrity of the JuliCA PKI;
- complying with legal, regulatory and contractual obligations; and
- responding to lawful requests from competent authorities.

Personal data collected by JuliCA is used for JuliCA-related services and is not used to provide unrelated services.

5. LAWFUL PROCESSING

JuliCA processes personal data only where permitted by applicable law.

Depending on the circumstances, processing may be undertaken where:

- the individual has given consent;
- processing is necessary for the performance of a contract or for taking steps at the request of the individual before entering into a contract;
- processing is necessary to comply with a legal or regulatory obligation;
- processing is necessary to protect the vital interests of an individual;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, where applicable; or
- processing is necessary for legitimate interests pursued by JuliCA, provided that such interests are not overridden by the rights and freedoms of the individual.

6. DATA PROTECTION PRINCIPLES

JuliCA shall process personal data in accordance with the following principles:

Lawfulness, fairness and transparency: Personal data shall be processed lawfully, fairly and transparently.

Purpose limitation: Personal data shall be collected for specific, explicit and limited purposes.

Data minimisation: Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.

Accuracy: Reasonable steps shall be taken to ensure that personal data is accurate and kept up to date where necessary.

Retention: Personal data shall not be retained for longer than necessary, subject to applicable legal, regulatory, audit and certification requirements.

Security and confidentiality: Personal data shall be protected against unauthorised access, disclosure, alteration, loss, destruction or other unlawful processing.

These principles reflect the data protection principles contained in JuliCA's existing Data Protection Policy.

7. ACCESS TO PERSONAL DATA

Access to personal data is restricted to authorised personnel who require such access to perform their duties.

Personal data shall not be informally shared or disclosed to persons who are not authorised to receive it. Personnel handling personal data are required to maintain its confidentiality and to use it only for authorised purposes.

8. SECURITY OF PERSONAL DATA

JuliCA maintains appropriate technical, organisational and physical measures to protect personal data against unauthorised access, accidental deletion, loss, destruction, alteration, disclosure and malicious activity.

These measures include, as appropriate:

- access controls and authorisation mechanisms;
- restricted access to personal data;
- strong passwords and protected credentials;
- encryption;

- secure servers and approved cloud services;
- firewalls and security software;
- physical security and access controls;
- regular backups;
- audit logging and monitoring;
- privilege management;
- vulnerability assessments and security testing;
- incident response procedures; and
- personnel training.

JuliCA requires electronically stored data to be accessible only to authorised personnel and requires appropriate measures to protect its systems and data.

Personal data transferred electronically shall be encrypted, and personnel shall not retain unauthorised copies of personal data on their individual devices.

9. CONFIDENTIALITY OF CERTIFICATION INFORMATION

JuliCA treats certain information processed in connection with its certification services as confidential.

Confidential information includes:

1. certificate applications;
2. records submitted in support of certificate applications;
3. private keys;
4. log files and other audit records; and
5. transaction records.

JuliCA, its contractors and agents are required to exercise reasonable care in processing and protecting confidential information.

Certificates and revocation data are not treated as confidential information under the JuliCA CPS and may be disclosed or made available in accordance with the applicable Certificate Policy, CPS and applicable requirements.

10. DISCLOSURE OF PERSONAL DATA

JuliCA shall not disclose personal data to unauthorised persons.

Personal data may be disclosed where necessary and lawful, including:

- to service providers processing information on behalf of JuliCA;
- to auditors and assessors;
- to professional advisers;
- to competent regulatory or governmental authorities;
- to law enforcement agencies where legally required or otherwise permitted;
- where necessary to investigate or prevent fraud, security incidents or unlawful activity; or
- where otherwise permitted or required by law.

Where a request for disclosure is received from a law enforcement authority, JuliCA shall take reasonable steps to confirm that the request is lawful before making the disclosure.

11. THIRD-PARTY SERVICE PROVIDERS

JuliCA may use third-party service providers to support its certification and trust services, including providers of hosting, technology, infrastructure, security, testing, technical support and other professional services.

Where a third party processes personal data on behalf of JuliCA, JuliCA shall take reasonable steps to ensure that the third party:

- processes the data only for authorised purposes;
- maintains appropriate confidentiality;
- implements appropriate security measures; and
- complies with applicable contractual and legal requirements.

12. INTERNATIONAL TRANSFERS

Where personal data is transferred outside Kenya or another jurisdiction in which it was collected, JuliCA shall take appropriate measures to ensure that the transfer is carried out in accordance with applicable data protection law.

Where required by applicable law, appropriate safeguards shall be implemented for the transfer of personal data.

13. RETENTION OF PERSONAL DATA

JuliCA shall retain personal data only for as long as necessary for the purposes for which it was collected, subject to legal, regulatory, contractual, audit and certification requirements.

Certain certification records are subject to specific retention periods. JuliCA retains audit logs for at least seven years, or longer where required by law.

JuliCA also retains documentation relating to certificate requests and their verification, certificates and revocation information for at least seven years after the relevant documentation ceases to be valid, or longer where required by law.

Accordingly, a request for deletion will not necessarily result in the immediate deletion of information where JuliCA is required to retain that information for legal, regulatory, audit, security or certification purposes.

14. DATA SUBJECT RIGHTS

Subject to applicable law and any lawful restrictions, individuals whose personal data is processed by JuliCA may have the right to:

- request access to personal data held about them;
- request information concerning the purposes for which their personal data is processed;
- request correction of inaccurate or incomplete personal data;
- request deletion of personal data where legally permissible;
- object to certain processing;
- request restriction of processing in applicable circumstances;
- withdraw consent where processing is based on consent; and
- exercise any other rights available under applicable data protection law.

JuliCA's existing data protection arrangements provide individuals with the right to ask what information is held about them, why it is held, how to access it, how to keep it up to date and how JuliCA meets its data protection obligations.

15. ACCESS AND CORRECTION REQUESTS

Requests for access to or correction of personal data may be submitted to JuliCA through the contact details provided in this Policy.

JuliCA may verify the identity of the person making a request before disclosing or modifying personal data.

JuliCA aims to respond to subject access requests within 14 days, subject to the nature and complexity of the request and applicable law.

16. ERASURE OF PERSONAL DATA

An individual may request the deletion of personal data where permitted by applicable law.

JuliCA shall consider each request in light of its legal, regulatory, contractual, audit, security and certification obligations.

Where information is required to be retained, JuliCA may decline or limit the request for deletion to the extent permitted by law.

17. CHILDREN'S DATA

JuliCA's website and services are not intended for children or persons under the age of 18.

JuliCA does not knowingly collect personally identifiable information from persons under 18. Where a parent or custodian believes that a person under 18 has provided personal information to JuliCA, they may contact JuliCA for the matter to be reviewed.

18. PERSONAL DATA BREACHES

JuliCA maintains procedures for identifying, responding to and managing information security incidents and personal data breaches.

JuliCA's incident response arrangements provide for the detection and investigation of cybersecurity incidents and data breaches, assessment of their scope and risk, appropriate response and communication with relevant stakeholders.

Where a personal data breach occurs, JuliCA shall assess the breach and take appropriate measures to contain, investigate and remediate the incident and make any notifications required by applicable law.

19. EMPLOYEE AND AUTHORISED PERSONNEL RESPONSIBILITIES

All JuliCA employees and collaborators are responsible for ensuring that personal data is collected, stored, handled and protected appropriately.

Personnel handling personal data shall:

- maintain confidentiality;
- access personal data only where authorised;
- use personal data only for legitimate and authorised purposes;
- protect passwords and credentials;
- prevent unauthorised disclosure or copying;
- comply with JuliCA's information security and data protection requirements; and
- report suspected misuse, unauthorised access or security incidents.

JuliCA provides training to personnel regarding their responsibilities when handling personal data.

20. DATA ACCURACY

JuliCA takes reasonable steps to ensure that personal data used in connection with its services is accurate and reliable.

Applicants and subscribers are responsible for providing accurate and complete information and for notifying JuliCA of relevant changes.

JuliCA may verify information provided for identification and authentication purposes and may reject applications where required information has not been provided or validated.

21. COMPLAINTS

Any individual who has a concern regarding the manner in which JuliCA processes personal data may raise the concern with JuliCA using the contact details provided in this Policy.

JuliCA shall review complaints and take appropriate action where a breach or deficiency is identified.

Nothing in this Policy prevents an individual from exercising any right to lodge a complaint with the relevant data protection supervisory authority under applicable law.

22. CHANGES TO THIS PRIVACY POLICY

JuliCA may amend this Privacy Policy from time to time to reflect changes in its services, systems, applicable law, regulatory requirements or data protection practices.

The current version of this Privacy Policy shall be made available through the appropriate JuliCA publication channels.

23. CONTACT INFORMATION

Questions, requests and concerns relating to this Privacy Policy or the processing of personal data by JuliCA may be submitted to:

JuliCA

Operated

by

TendaWorld

Limited

Nairobi, Kenya

Email: mail@tenda.world

24. GOVERNING LAW

This Privacy Policy shall be governed by and interpreted in accordance with the laws of Kenya, including the Data Protection Act, 2019, together with applicable regulations and other applicable legal and regulatory requirements.

Where the EU GDPR or another foreign data protection law applies to particular processing activities, JuliCA shall comply with the applicable requirements to the extent required by law.

DOCUMENT CONTROL

Document	JuliCA Privacy Policy
Version	1.0
Effective Date	27 March 2026
Owner	JuliCA
Review Frequency	At least annually and whenever material changes occur
Related Documents	JuliCA Certificate Policy; JuliCA Certification Practice Statement; Data Protection Policy; Incident Response Plan; IT Security Policy; Business Continuity Plan; Disaster Recovery Plan