DocinVault

TRUST AND IDENTITY PROOFING

Trust Service Practice Statement and Identity Proofing Service Practice Statement

Practices governing DocinVault identity-proofing components when they are used in regulated, contractual, or trust-service workflows.

VERSION	EFFECTIVE	OWNER
5	May 28, 2026	DocinVault

Purpose and status

This Trust Service Practice Statement and Identity Proofing Service Practice Statement describes the practices DocinVault LLC applies when providing configurable remote identity-proofing components. It supports customer due diligence, contractual review, and the identity-proofing requirements used in electronic trust-service workflows, including workflows supporting issuance of qualified certificates.

DocinVault provides real-time identity verification through computers, mobile devices, supported mobile applications, APIs, and web interfaces. The service combines NFC and OCR document reading, facial similarity, active and passive liveness, spoof detection, video verification, review, screening, result delivery, and a management console. A customer or trust service provider determines the purpose, assurance target, accepted evidence, legal basis, decision rules, and reliance model for its implementation.

> **Important service boundary**
>
> DocinVault provides the identity-proofing aspects needed to support qualified-certificate issuance but does not issue certificates or provide the other certification services governed by a complete Certification Practice Statement. The issuing trust service provider remains responsible for its certificate policy, authorization, issuance decision, and regulated trust-service obligations.

Company details

Service provider	DocinVault LLC
Registered address	43 Meskheti St., Borjomi, Georgia
Website	https://docinvault.com
General contact	contact@docinvault.com
Privacy and legal contact	legal@docinvault.com

Contents

SECTION 01

Scope and service boundaries

This statement covers the practices used to deliver the following configurable capabilities:

- browser-based and customer-initiated identity-verification sessions;
- identity-document capture or upload, and NFC-derived data where configured and supported;
- document quality, validity, consistency, and configured authenticity checks;
- facial similarity, active or passive liveness, and manual-review paths;
- Video KYC, proof-of-address, AML, KYB, age, questionnaire, and transaction-monitoring modules where configured;
- structured results, workflow statuses, audit events, API delivery, and webhooks; and
- hosted operational tools used to create sessions, configure master and authorized sub-accounts, and review configured outcomes; and
- electronic delivery of identity-proofing results to contracted relying parties or trust service providers supporting qualified-certificate issuance.

This statement does not define a certificate policy, certificate-issuance lifecycle, electronic-signature creation service, electronic-seal service, timestamping service, or the practices of a third-party trust service provider. Those services remain outside scope unless a separate written agreement and applicable authorization expressly include them.

Customer-specific agreements, data processing terms, technical specifications, and configuration records may supplement this statement. Where a signed agreement imposes a more specific requirement, that requirement controls for the relevant deployment.

SECTION 02

Applicable framework and references

DocinVault uses the following materials as relevant design and control references. The applicable version, jurisdiction, assurance level, and conformity obligation depend on the customer's use case and contract.

- Law of Georgia on Personal Data Protection;
- Law of Georgia on Electronic Documents and Electronic Trust Services;
- Regulation (EU) 2016/679, the General Data Protection Regulation, where applicable;
- Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, where applicable;
- ETSI EN 319 401, General policy requirements for trust service providers;
- ETSI EN 319 411-1 and ETSI EN 319 411-2, policy and security requirements for trust service providers issuing certificates;
- ETSI EN 319 411-3, policy and security requirements relevant to certificate services and electronic seals;
- ETSI EN 319 403, requirements for conformity assessment of trust service providers and trust services;
- ETSI TS 119 461 V2.1.1, policy and security requirements for trust service components providing identity proofing of trust service subjects; and
- ISO/IEC 30107-3, biometric presentation attack detection testing and reporting;
- ISO/IEC 27001, information security management systems; and
- SOC 2 Trust Services Criteria for security, availability, processing integrity, confidentiality, and privacy.

> **Interpretation**
>
> Listing a law or standard as a reference does not represent certification, authorization, or universal conformity. A certification or testing claim applies only to the product, version, scope, period, and report identified by the supporting evidence.

SECTION 03

Roles and definitions

Term	Meaning in this statement
Applicant	The natural person completing an identity-proofing session.
Customer	The organization that configures, requests, or relies on a DocinVault workflow.
Identity attribute	Information associated with a person, such as name, date of birth, nationality, address, or document details.
Identity evidence	A document, image, video, electronic attribute, or other evidence presented to support an identity claim.
Identity proofing	The process of collecting, validating, and binding evidence to an applicant and issuing a result to the authorized relying organization.
Liveness	A check intended to assess whether biometric evidence is being obtained from a live person present during capture.
Relying party	An authorized organization that uses an identity-proofing result for its stated purpose.
Session record	The configured result, evidence references, workflow events, timestamps, and audit information associated with a session.

When DocinVault processes personal data for a customer-controlled workflow, the customer normally acts as controller and DocinVault acts as processor or service provider. The applicable agreement and data-processing notice determine the exact roles.

SECTION 04

Identity-proofing context

The identity-proofing context is the combination of legal, operational, fraud, and assurance requirements that apply to a workflow. It determines which applicants are in scope, which evidence is accepted, what checks are performed, what level of human review is required, what result may be relied on, and how long evidence is retained.

Market and purpose variation

Document types, required attributes, reporting fields, legal bases, access rules, and retention periods differ by market and purpose. DocinVault therefore configures workflows market by market and does not represent that one configuration satisfies every jurisdiction.

Depending on the governing assurance policy and selected controls, DocinVault supports identity-proofing configurations designed for substantial or high levels of assurance. Core evidence can include passports, national identity cards, and driving licences capable of uniquely identifying an applicant. Additional supported evidence is documented in the published Issuing Countries catalog. Optional authoritative-source checks, including lost, stolen, or revoked document databases such as Interpol or an available national register, may be configured by the customer.

Customer configuration

The customer is responsible for defining and approving, as applicable:

- the purpose of identity proofing and the relevant applicant population;
- accepted document types, capture channels, and authoritative sources;
- required identity attributes and the minimum necessary output;
- liveness method, similarity thresholds, retry rules, and manual-review ranges;
- decision, escalation, reporting, and exception procedures;
- authorized roles and downstream recipients;
- retention, deletion, and evidence-access rules; and
- the legal basis and notice presented to applicants.

Presentation attack detection mechanisms are tested by accredited laboratories against representative datasets under ISO/IEC 30107-3. Relevant performance metrics may include APCER, BPCER, IAPMR, FMR, and FNMR for the tested component and attack instrument scope.

SECTION 05

Identity-proofing lifecycle

Step 01

Initiation

A customer or authorized user creates a session through a hosted portal, API, webhook, or another approved integration path. The session identifies the configured workflow and presents the applicable notice and instructions to the applicant.

Step 02

Attribute and evidence collection

The applicant provides only the evidence required by the workflow. This may include an identity document, proof of address, selfie image, selfie video, live video, questionnaire response, or configured electronic document data. Capture-quality checks may request a retry when evidence is unreadable, incomplete, or unsuitable.

Step 03

Attribute and evidence validation

Configured checks may assess document type, visible fields, expiry, consistency, image quality, MRZ data, NFC-derived data, document security signals, or configured authoritative sources. Availability varies by document, market, device, and customer configuration.

Step 04

Binding evidence to the applicant

Facial similarity and liveness checks may be used to assess whether the person presenting the evidence corresponds to the document portrait and is present during the session. Active, passive, or review-based methods depend on configuration.

Step 05

Decision and review

A session can produce a configured status, such as approved, rejected, pending, or needs review. Thresholds and routing rules may support automated decisions, manual review, or a combination. The customer determines how a status affects its own process.

Step 06

Issuance of proof

DocinVault returns the configured verification status, structured fields, and relevant audit events through the authorized portal, API, or webhook. Raw document access is restricted and is not part of the default minimum output unless the workflow and applicable law require it.

Normalization, evidence quality, and session status

OCR-derived identity text is normalized using Unicode Normalization Form C and case folding. Diacritics are retained in the canonical value and a diacritic-stripped variant may support tolerant comparison where names are truncated, initials are used, or components are missing. Captured image or video quality is evaluated for lighting, reflection, blur, and sharpness. Unusable evidence is rejected with retry guidance, and the customer configures the available retry count.

Document validation may include SOD certificate validation, electronic-seal or chip integrity, document-type and side requirements, and configured statuses such as APPROVED, REJECTED, or MANUAL_CHECK. Evidence records include the document, captured images, status, completion time, and applicable qualified timestamp where configured.

SECTION 06

Configured verification methods

Document capture
Camera capture, controlled upload, or NFC-supported collection may be enabled according to the workflow and supported device.

Document assessment
Quality, expiry, field consistency, MRZ, NFC, and configured security-signal checks may be combined. No single check is treated as universally conclusive.

Facial similarity
Configured comparison methods assess correspondence between applicant evidence and an identity-document portrait, subject to thresholds and review rules.

Liveness
Active or passive liveness methods may be used to detect presentation attacks and confirm live presence during the configured flow.

Video KYC
A live or recorded video workflow may support guided evidence presentation, reviewer interaction, and audit evidence where the customer requires it.

Manual review
Configured cases can be routed to authorized reviewers. Review criteria, permissions, training, and final reliance remain subject to customer policy and contract.

Document fraud controls
MRZ integrity, expiry, manipulated-photo, device-screen, blur, brightness, ghost-image, black-and-white copy, font, template, and front-to-back consistency controls can be combined.

Biometric binding
Facial comparison produces a configurable similarity score. The transient biometric vector map used for comparison is deleted immediately after the similarity level is established.

Presentation attack detection
Passive, cascading, and dynamic-selfie liveness may be combined with gaze, flat-surface, 3D-mask, and silicone-mask detection.

Video verification
Live video captures the applicant with the presented document, supports document images from both sides, and applies paper-image and screen-presentation detection.

SECTION 07

Results, evidence, and audit history

DocinVault is designed to provide the minimum result and structured fields required for the authorized workflow. The exact output depends on configuration and may include session status, verified attributes, check outcomes, reason codes, review state, timestamps, and workflow events.

Audit history may record session creation, evidence collection, check execution, result changes, authorized access, review actions, and delivery events. Audit evidence supports accountability but does not by itself establish legal compliance or replace the relying party's own records.

Access to session records is limited to authorized roles and approved integration paths. Customers must configure permissions according to least-privilege and operational need. Download or disclosure of raw identity evidence must be separately justified, controlled, and logged where enabled.

The management console and API can provide millisecond-accurate session logs, captured attributes, verification outcomes, review history, and recorded video where the workflow requires it. Session activities, access, and modifications are logged and protected using SHA-256 hashing. Stored session data is encrypted, and the complete audit trail remains available to authorized customer users for configured review, download, and compliance purposes.

SECTION 08

Data protection and retention

Data minimization

Workflows should collect only evidence and attributes needed for the stated purpose. DocinVault supports configurable outputs so operational teams can receive a status and selected fields instead of unrestricted document copies by default.

Transparency and lawful basis

The controller must provide an appropriate notice and identify a lawful basis before processing begins. Where biometric data is used for unique identification, the controller must also identify any additional condition required for special-category data under applicable law.

Retention and deletion

Verification evidence is retained according to the customer's documented instructions, configured period, contract, and applicable law. The biometric vector map used for facial similarity is deleted immediately after the similarity level is established. Anonymized technical and security logs are retained for three years to support auditability, reliability, security investigation, and legal obligations. At the end of any other applicable period,

data is deleted or de-identified unless continued retention is legally required or necessary for a documented legal claim.

Data-subject rights

DocinVault supports customers in responding to lawful requests for access, correction, deletion, restriction, objection, portability, and review where those rights apply. Applicants should normally contact the organization that requested the verification. Privacy inquiries may also be sent to legal@docinvault.com.

International transfers and subprocessors

Cross-border transfers and subprocessors must be governed by appropriate contractual, security, and legal safeguards. The deployment agreement or dedicated notice identifies applicable providers and transfer arrangements where disclosure is required.

SECTION 09

Governance, personnel, and assets

DocinVault maintains an information security framework covering confidentiality, integrity, availability, acceptable use, asset management, backup, classification, encryption, incident response, teleworking, cloud computing, and secure handling of information in every supported medium. The framework is reviewed regularly against business risk, legal obligations, customer commitments, and applicable standards.

Risk management
A SOC 2-aligned risk process identifies threats and vulnerabilities, evaluates likelihood and impact, applies a risk matrix, defines risk appetite, and tracks treatment through a Plan of Action and Milestones.

Oversight
The Board and executive functions oversee governance. The Information Security Manager and Information Security Management Committee coordinate risk, while operational and legal leaders maintain security and regulatory accountability.

Personnel security
Employees and contractors are subject to background checks where lawful, confidentiality obligations, role-based training, disciplinary rules, secure role changes, tracked offboarding, and clean-work-area requirements.

Asset management
Physical and virtual assets receive owners, classifications, lifecycle controls, inventory records, and unique identifiers. DocinVault uses Drata to support tracking of systems, virtual machines, user accounts, and compliance evidence.

Media handling
Media is protected during storage and transfer, disposed of through documented sanitization appropriate to its classification, and handled so removed data cannot reasonably be retrieved or reconstructed.

Access control
Unique identities, role-based access, least privilege, strong password and session controls, periodic review, cloud access restrictions, workstation encryption, firewalls, and prompt account removal protect systems and data.

SECTION 10

Encryption, physical security, and infrastructure

Cryptographic controls

DocinVault uses AES-256 for protected data encryption and applies cryptographic controls to VPN keys and cloud services. Managed key processes govern generation, storage, rotation, distribution, access, loss prevention, symmetric and public-key use, and retirement. Session activity and evidence integrity are also protected using SHA-256 hashing where described in the service design.

Physical and environmental security

Physical security perimeters, fingerprint or badge readers, smart locks, visitor logs and escorts, monitored entry points, alarms, controlled reception, protected off-site equipment, cabling safeguards, environmental controls, and backup power protect DocinVault-controlled facilities and assets. Cloud providers govern physical data-center controls under their assurance programs and agreements.

Processing locations and providers

Provider	Location and function	Contractual safeguards
Amazon Web Services EMEA SARL	38 Avenue John F. Kennedy, L-1855 Luxembourg. Primary cloud infrastructure and processing.	AWS data processing agreement, GDPR terms, and updated Standard Contractual Clauses where required.
Google Cloud EMEA Limited	70 Sir John Rogerson's Quay, Dublin 2, Ireland, with relevant servers in Frankfurt, Germany. Backup and restoration services for the AWS environment.	Google Cloud data processing terms, GDPR safeguards, and updated Standard Contractual Clauses where required.
Cloudflare, Inc.	101 Townsend St, San Francisco, CA 94107, USA. Traffic routing, security, availability, and processing of network interaction data such as IP address, routing, traffic, and system configuration information.	Cloudflare contractual privacy, security, and international-transfer terms.

SECTION 11

Operational security and incident response

Secure development lifecycle

The software development lifecycle covers authorization, requirements, secure design, implementation, readiness review, testing, and deployment. Controls include separation of duties, secure programming standards, protected development environments, developer security training, interoperability controls, data portability, secure APIs, change review, and compliance with legal and contractual requirements.

Network and vulnerability management

Product systems undergo vulnerability scanning and penetration testing at least annually. Automated security agents and external tools are kept current, audit activities are controlled and logged, and findings are assigned Critical, High, Medium, or Low priority with remediation service levels. No release enters production with unresolved Critical or High findings unless the Security Manager and affected asset owner approve a documented exception and compensating controls.

Incident management and notification

The incident response process covers detection, reporting, containment, investigation, risk assessment, forensic preservation, corrective action, cloud-provider coordination, documentation, and communication. Personnel, contractors, and external users are required to report suspected security incidents or vulnerabilities within 24 hours.

If an incident affects a customer's use of DocinVault services, DocinVault notifies the affected customer without undue delay and no later than 24 hours after detection. Available information includes the nature and scope, initial impact assessment, and mitigation measures so the customer can meet its own regulatory duties.

SECTION 12

Continuity, insurance, and termination

Business continuity and disaster recovery

The Business Continuity Plan and Disaster Recovery Plan use risk assessment, vulnerability analysis, and business impact analysis to prioritize systems and recovery actions. Controls are maintained at primary and backup locations and tested annually. Lines of succession, response teams, remote-work or relocation options, application recovery, resource requirements, and customer updates through a status page support continued operation during disruption.

Liability and insurance

Liability limits and remedies are governed by individual customer agreements. DocinVault maintains General Liability insurance, including for applicable cases where a contractual limitation of liability does not apply.

Termination planning

The termination plan covers stakeholder notification, revocation of subcontractor authorizations, secure destruction of sensitive data and private keys, preservation or transfer of required audit logs and verification records, and feasible transition of identity-proofing services to another provider under an appropriate service level. Financial provisions support orderly termination and reduce bankruptcy or incapacity risk.

SECTION 13

Assurance evidence and compliance audits

As of the effective date, the product owner has approved publication of the following DocinVault evidence and marks. Each item must be interpreted according to its supporting report, tested component, scope, and validity period.

- iBeta Level 1 and Level 2 ISO/IEC 30107-3 presentation attack detection marks;
- BixeLab presentation attack detection testing;
- Praetorian security testing;
- ISO/IEC 27001 information security management certification;
- SOC 2 Type 2 mark;
- eIDAS compliant mark;
- GDPR compliant mark; and
- CCPA compliant mark.

External assessment cycle

DocinVault is subject to regular independent external audits under the eIDAS framework and applicable ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, and ETSI TS 119 461 requirements. Full conformity assessments are performed at least every 24 months, with a surveillance audit 12 months after each full audit and additional assessment following substantial system, configuration, or process changes that may affect service security.

Audit results are documented and archived and may be released to auditors, customers, or competent authorities as appropriate. Identified deficiencies result in a corrective action plan developed by management with the auditor and Information Security Management Committee. Immediate threats receive an agreed accelerated correction timetable, while lower-risk findings are evaluated and addressed proportionately.

SECTION 13 CONTINUED

> **Evidence scope**
>
> A mark or report does not certify every DocinVault module, customer configuration, jurisdiction, or relying-party process. Customers should request the supporting evidence needed for their review and confirm that its scope matches the intended deployment.

SECTION 14

Customer responsibilities and reliance

Customers and relying parties are responsible for:

- confirming that the selected workflow is lawful and proportionate for its purpose;
- providing required notices and identifying the applicable legal basis;
- selecting appropriate assurance, evidence, threshold, retry, and review settings;
- limiting access and downstream disclosure to authorized recipients;
- reviewing exceptions and not treating an automated status as an infallible determination;
- maintaining any records or reporting required by the customer's law or regulator;
- responding to applicants and data-subject requests as controller; and
- monitoring changes to local law, accepted documents, and authoritative sources.

An identity-proofing result is evidence produced by the configured process. It is not legal advice, a guarantee of identity, or a universal authorization to grant access, issue a certificate, complete a transaction, or satisfy a reporting duty. The relying party must evaluate the result in its own risk and legal context.

Liability, warranties, service levels, and remedies are governed by the applicable signed agreement. Nothing in this statement excludes an obligation or liability that cannot lawfully be excluded.

SECTION 15

Statement management and contact

Statement management

This statement is reviewed periodically through management and information-security governance and whenever a material product, legal, standards, configuration, or control change affects its content. The published version number and effective date identify the controlling public copy. Historical copies and review evidence are retained for accountability.

Contact

Questions about this statement, assurance evidence, or customer due diligence may be sent to contact@docinvault.com. Privacy and legal questions may be sent to legal@docinvault.com.

DocinVault LLC

43 Meskheti St., Borjomi, Georgia

Version 5, effective May 28, 2026

APPENDIX A

Identity-proofing lifecycle mapping

ETSI TS 119 461 lifecycle area	DocinVault practice summary	Primary evidence
Initiation	Customer-created session, configured notice, applicant instructions, and workflow identifier.	Session creation event, configuration record, notice version.
Attribute and evidence collection	Configured document, biometric, address, questionnaire, video, or electronic evidence with quality handling.	Capture events, evidence references, retry events, applicant inputs.
Attribute and evidence validation	Configured quality, validity, consistency, MRZ, NFC, security-signal, screening, or authoritative-source checks.	Check outcomes, source response where applicable, reason codes.
Binding to applicant	Configured facial similarity, liveness, video, and manual-review controls.	Similarity or liveness outcome, review event, threshold configuration.
Issuance of proof	Authorized delivery of status, structured fields, reason codes, and audit events through portal, API, or webhook.	Final status, delivery event, audit history, authorized recipient.

This mapping is descriptive. The customer and any regulated trust service provider must determine whether the selected configuration and evidence satisfy the assurance policy, certificate policy, and applicable law for the intended use.