

Security Overview

How DocReveal protects your documents and data • Effective from 26 September 2026

Provider	DocReveal s.r.o., ID No. 29871972, Příčná 1892/4, 110 00 Praha 1, Czech Republic
Applies to	DocReveal web application (app.docreveal.ai), its API and MCP access
Binding measures	Section 9 of the Data Processing Terms (DPA); this overview describes how they are implemented
Security contact	info@docreveal.org • Support Center in the web application

1. Purpose of this document

This Security Overview describes the technical and organisational measures that DocReveal applies to protect the DocReveal Services. It supplements Section 9 of the Data Processing Terms (DPA), available at <https://docreveal.ai/assets/documents/legal/docreveal-dpa-en.pdf>, which lists the measures DocReveal is contractually committed to, and Section 2.11 of the Terms of Service. DocReveal may update the measures described here, provided that the overall level of security is not reduced (Section 9.2 of the DPA).

2. Infrastructure and data location

- The Services run on a serverless architecture on Amazon Web Services (AWS). User Data are stored and processed in the European Union – primarily in the Stockholm region (eu-north-1); other EU regions may be used for redundancy and AI inference.
- AWS data centres are certified to ISO/IEC 27001 and audited under SOC 2 Type II. Certificates and reports are provided on request to the extent DocReveal is entitled to disclose them (Section 14.1 of the DPA).
- AI models are used through Amazon Bedrock within the EU. The model providers (such as Anthropic) do not receive User Data and do not use them for training, and DocReveal does not use User Data or Outputs to train general-purpose AI models.
- Optional tools (maps, web search, company registers) send only the query to their provider and only when they are used. All Sub-processors are listed in the Sub-processor List at <https://docreveal.ai/assets/documents/legal/docreveal-subprocessors-en.pdf>.

3. Encryption

- **In transit:** HTTPS with TLS 1.2 or higher for all connections between users and the Services (enforced as the minimum protocol on the content delivery network) and between the components of the Services.
- **At rest:** stored data are encrypted with industry-standard algorithms; encryption keys are managed by the AWS key management service.
- **Secrets:** credentials of integrations and other secrets are kept in a managed secret store (AWS Secrets Manager), not in the application code.

4. Tenant isolation and access control

- Each customer environment (tenant) is logically separated from the environments of other customers. Every request is authorised on the server side against the user's tenant, role and permissions.
- Access within a workspace is governed by roles and permissions and is enforced at the level of the individual document (role- and attribute-based access control).
- Access by DocReveal personnel to customer data is limited to the minimum necessary, based on the principles of least privilege and need-to-know, and is logged.

5. Authentication and sessions

- Registration and sign-in exclusively with an e-mail address and a password, with confirmation of registration by e-mail. Passwords are stored only as salted hashes by the identity service (Amazon Cognito); sign-in through third-party identity providers is not offered.
- The browser holds only a random session identifier in an httpOnly and Secure cookie with the SameSite attribute; a session expires after 60 minutes of inactivity.
- Requests that change data are protected against cross-site request forgery (CSRF tokens), and sign-in and the API are protected by rate limiting against brute-force attempts and abuse.
- API keys issued by DocReveal (for example for MCP access) are displayed only once and stored only as hashes.
- DocReveal's administrative access to the infrastructure is protected by multi-factor authentication.

6. Application and infrastructure security

- Public endpoints are protected by a web application firewall and by the DDoS protection of the cloud provider.
- Uploaded files are checked for file type and size before they are processed.
- Tools that open web pages are protected against server-side request forgery: only public HTTPS addresses are allowed, the target is verified after DNS resolution and the size of the response is limited.
- Container images are scanned for known vulnerabilities; dependencies are patched and updated regularly.
- Changes are tested with automated test suites and approved before they are deployed to production.

7. Logging, monitoring and audit

- Access to data and operations performed on data – including the steps of AI processing and the queries submitted to the AI Features – are recorded in an audit trail.
- Application and infrastructure logs are kept in the managed logging service of the cloud provider (Amazon CloudWatch) with restricted access and protection against modification. Security and operational logs are retained as a rule for 12 months.
- Operation of the Services is monitored, including errors and the health of the document processing pipelines.

8. Availability, backups and deletion

- The serverless infrastructure of the cloud provider is redundant across availability zones. The target availability of the Services is at least 90 % per calendar month (Section 2.10 of the Terms of Service).
- DocReveal does not create backups of User Data on behalf of the User. Users can export their data at any time and can set up continuous backups to their own environments through the integrations in the web application.
- Technical recovery copies kept within the infrastructure for operational resilience (database point-in-time recovery and previous versions of stored objects) cannot be used to restore data at the User's request and are automatically erased no later than 35 days after the deletion.
- Deleting a workspace deletes all User Data, all data derived from them (such as vector embeddings, search indexes and graph entities), conversations, configuration and integration credentials (Section 12.3 of the Terms of Service).

9. Incident management

- DocReveal maintains a documented procedure for detecting, classifying, resolving and reporting security incidents and personal data breaches.
- Users are notified of a personal data breach affecting their data without undue delay and no later than 48 hours after DocReveal becomes aware of it (Section 12 of the DPA).

10. Organisational measures

- Information security policies approved by management and reviewed at least annually.
- Confidentiality obligations for all personnel and contractors with access to Personal Data, surviving the end of their engagement, and security awareness training.
- Access management based on least privilege and need-to-know, with regular review of access rights and immediate revocation when a role ends.
- Assessment of Sub-processors before they are engaged and contractual data protection obligations equivalent to those in the DPA.

11. Shared responsibility

Security is shared between DocReveal and its users. Users are responsible in particular for:

- managing users, roles and access rights in their workspace and revoking access that is no longer needed;
- keeping passwords and API keys confidential and reporting suspected misuse without delay;
- uploading only data they are entitled to process and reviewing AI Outputs before relying on them;
- exporting data they wish to keep before deleting documents or the workspace;
- not attempting to bypass the security or access controls of the Services (Section 2.5 of the Terms of Service).

12. Reporting a vulnerability or incident

Contact

Report suspected vulnerabilities or security incidents to **info@docreveal.org** or through the Support Center in the web application. Please do not access or change data that does not belong to you, agree any security testing with us in advance and give us reasonable time to fix an issue before disclosing it.

Related documents: the Terms of Service, Privacy Policy, Data Processing Terms (DPA) and information under the Data Act are linked in the footer of docreveal.ai; the Sub-processor List is linked from Section 10.2 of the DPA. Last updated: 26 September 2026.