

LEGAL

Technical and organisational measures

The measures Sovaro GmbH takes under Art. 32 GDPR to protect the files customers submit to PreVDR. This document is Annex 3 of the Data Processing Agreement (<https://www.prevdr.com/legal/dpa>).

Last updated: 15 October 2026

1. Approach

The most effective protection for a document is not to keep it. PreVDR therefore processes files transiently: each file exists on our infrastructure only while it is compressed, verified and downloaded, and is then deleted automatically. There are no user logins, no document storage, no archive and no history. The measures below build on this principle, having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing.

2. Infrastructure and physical security

- The PreVDR service and the Claude language models it uses (provided through Amazon Bedrock) run on Amazon Web Services in the region Europe (Frankfurt), eu-central-1, Germany.
- This infrastructure is ISO/IEC 27001 certified and BSI C5 attested; AWS also publishes SOC 2 reports. These are certifications of AWS, not of Sovaro.
- Sovaro does not operate its own data centres or server rooms. Physical access control, power supply, cooling, fire protection and hardware disposal are the responsibility of AWS under its contractually agreed security measures.

3. Transient processing and deletion

- Uploaded files and results are held only in the processing environment on AWS in Frankfurt and are deleted automatically as soon as processing and download are complete, at the latest 15 minutes after processing.
- Sovaro keeps no copies, archives or backups of customer files. Deleted files cannot be restored, by Sovaro or by anyone else.
- Each upload is processed as a separate job under a random identifier. Files of different jobs are kept apart, and a result can be retrieved only with the identifier of its own job.
- Amazon Bedrock does not store or log the content sent to the language models or the content they return, and does not use it to train models. Anthropic, the provider of the models, has no access to customer files.

- Sovaro does not use customer files for training, analysis or any purpose other than the requested compression.

4. Encryption and transmission

- All connections between the browser, the website and the PreVDR service are encrypted with TLS 1.2 or higher; TLS 1.3 is used where the client supports it.
- The website relays requests to the PreVDR service through a fixed list of permitted routes. Requests outside this list are rejected without reaching the service. The relay passes data through without storing it.
- The relay authenticates itself to the PreVDR service with a secret key, so the service accepts uploads only through the website.
- Storage used by the processing environment on AWS is encrypted at rest with AES-256.

5. Access control

- Administrative access to the AWS environment is restricted to the few persons at Sovaro who need it to operate the service, with personal credentials.
- Secrets such as access keys are kept in the configuration of the hosting environments and never in the source code.
- Sovaro staff do not open or view customer files in the course of operating the service.
- Logs record technical events (for example time, file size and type, processing duration and error codes) but never file content or file names.
- Per-network rate limits and limits on file size, queue length and concurrent processing protect the service against misuse and overload.

6. Integrity: verification of every result

Before a result is offered for download, PreVDR compares it with the original file:

- PDF files: every page is rendered and compared pixel by pixel; the text and the document structure are checked.
- Word, Excel and PowerPoint files: every part of the file is compared using SHA-256 fingerprints.
- PNG and JPEG images: compared pixel by pixel.
- If any difference is found, or a file cannot be reduced, the customer receives the original file unchanged.

7. Availability and resilience

- Because the customer keeps its original files and PreVDR stores nothing, an interruption of the service can delay processing but cannot cause the loss of stored customer documents.
- The infrastructure of AWS in Frankfurt provides redundant power, cooling and network connections.
- Limits on queue length and concurrent processing keep the service stable under load.

8. Organisational measures

- Everyone at Sovaro who may come into contact with customer data commits in writing, before starting, to confidentiality and to data secrecy under § 6 DSG, and is informed of the professional secrecy provisions of § 121 of the Austrian Criminal Code, § 203 of the German Criminal Code and Art. 321 of the Swiss Criminal Code.
- Subprocessors are engaged only under data processing agreements under Art. 28 GDPR. The current list is Annex 2 of the Data Processing Agreement.
- Professionals bound by secrecy can conclude a separate confidentiality agreement with Sovaro (www.prevdr.com/legal/confidentiality).

9. Incident response

- Security incidents are assessed without undue delay after they become known, contained and documented.
- Customers affected by a personal data breach are informed without undue delay, so that they can meet their own notification obligations within 72 hours (section 10 of the Data Processing Agreement).
- Security concerns can be reported at any time to office@prevdr.com.

10. Regular review

- Sovaro reviews these measures at least once a year and whenever the service, the subprocessors or the risks change, and updates this document accordingly.
- Changes never reduce the level of protection described here. The date at the top shows the current version.