

LEGAL

Data Processing Agreement

This agreement under Art. 28 of the General Data Protection Regulation (GDPR) governs how Sovaro GmbH processes personal data contained in the files a customer submits to PreVDR. It forms part of every contract for the PreVDR service.

Last updated: 15 October 2026

Parties and background

This Data Processing Agreement ("DPA") is concluded between the customer named in the Access Confirmation ("Customer") and Sovaro GmbH, Weißgerberlande 60/23, 1030 Vienna, Austria, FN 651695 a, Handelsgericht Wien ("Sovaro"). It supplements the General Terms and Conditions for PreVDR (www.prevdr.com/legal/terms) and any other agreement on the use of PreVDR (together, the "Agreement").

When the Customer submits files to PreVDR, those files may contain personal data. Sovaro processes such data only to compress the files and return them to the Customer. This DPA sets out the rights and obligations of both parties for this processing.

1. Definitions

- 1.1 Terms such as "personal data", "processing", "controller", "processor", "data subject" and "personal data breach" have the meaning given to them in Art. 4 GDPR.
- 1.2 "Customer Data" means all personal data contained in the files the Customer or its users submit to PreVDR, and in the files returned by PreVDR, which Sovaro processes on behalf of the Customer.
- 1.3 "Data Protection Law" means the GDPR, the Austrian Data Protection Act (DSG) and any other data protection law applicable to the processing under this DPA.
- 1.4 "Subprocessor" means a further processor engaged by Sovaro that processes Customer Data.
- 1.5 "Service" has the meaning given to it in the General Terms and Conditions.

2. Subject matter, nature and duration

- 2.1 Subject matter, nature and purpose of the processing, the types of personal data and the categories of data subjects are described in Annex 1.

- 2.2 Sovaro processes Customer Data transiently: each file is held only for as long as processing, verification and download require, and is deleted automatically no later than 15 minutes after processing. Sovaro keeps no copies, archives or backups of Customer Data.
- 2.3 This DPA applies for as long as Sovaro processes Customer Data under the Agreement. It ends automatically when the Agreement ends, but its provisions continue to apply for as long as Sovaro still holds any Customer Data.

3. Roles of the parties

- 3.1 The Customer is the controller of Customer Data. Sovaro processes Customer Data as a processor on behalf of the Customer.
- 3.2 Where the Customer itself processes the data on behalf of a third party (for example an advisor acting for its client), the Customer is the processor and Sovaro is its further processor. In this case the Customer warrants that the controller has authorised the engagement of Sovaro, and the Customer passes on the controller's instructions.
- 3.3 The Customer is responsible for the lawfulness of the processing, in particular for having a legal basis for submitting Customer Data to the Service and for informing data subjects.

4. Instructions

- 4.1 Sovaro processes Customer Data only on documented instructions from the Customer, unless Union or Member State law requires otherwise; in that case Sovaro informs the Customer of the legal requirement before processing, unless the law prohibits this.
- 4.2 The Agreement, this DPA and the Customer's use of the Service (submitting files and downloading the results) constitute the Customer's complete instructions at the time this DPA is concluded. Further instructions must be given in text form to office@prevdr.com and must be technically feasible within the Service.
- 4.3 Sovaro informs the Customer without undue delay if it considers that an instruction infringes Data Protection Law. Sovaro may suspend carrying out such an instruction until the Customer confirms or changes it.
- 4.4 Sovaro does not use Customer Data for its own purposes, in particular not to train or improve language models, not for analysis and not for advertising.

5. Confidentiality of personnel

- 5.1 Sovaro ensures that every person authorised to process Customer Data has committed in writing to confidentiality and to data secrecy under § 6 DSG, and is informed of the applicable professional secrecy provisions, in particular § 121 of the Austrian Criminal Code (StGB), § 203 of the German Criminal Code (StGB) and Art. 321 of the Swiss Criminal Code (StGB). These obligations continue after the end of their activity.

- 5.2 Sovaro staff do not view the content of Customer Files in the course of normal operation. Access to the systems that process Customer Data is limited to the persons who need it to operate the Service.

6. Security of processing

- 6.1 Sovaro implements the technical and organisational measures described in Annex 3 to ensure a level of security appropriate to the risk (Art. 32 GDPR).
- 6.2 The measures are subject to technical progress. Sovaro may replace them with adequate alternative measures, provided the level of protection is not reduced. Sovaro documents material changes and updates Annex 3 accordingly.

7. Subprocessors

- 7.1 The Customer authorises Sovaro to engage the Subprocessors listed in Annex 2.
- 7.2 The Customer grants Sovaro a general authorisation to engage further Subprocessors or replace existing ones. Sovaro informs the Customer of any intended change in text form at least 30 days in advance. The Customer may object to the change in text form within this period on reasonable data protection grounds. If Sovaro does not address the objection, the Customer may terminate the Agreement with effect from the date the change takes effect.
- 7.3 Sovaro imposes on each Subprocessor data protection obligations that offer at least the same level of protection as this DPA, in particular sufficient guarantees for appropriate technical and organisational measures. Sovaro remains liable to the Customer for the performance of the Subprocessor's obligations.
- 7.4 Services that Sovaro uses as ancillary services without access to Customer Data, for example telecommunications or network providers merely transmitting encrypted data, are not Subprocessors within the meaning of this section.

8. Location of processing and transfers to third countries

- 8.1 The Service, including the Claude language models by Anthropic provided through Amazon Bedrock, runs on Amazon Web Services in the region Europe (Frankfurt), eu-central-1, Germany. Customer Data is compressed and verified there. Amazon Bedrock does not pass Customer Data to the model provider: Anthropic has no access to it.
- 8.2 Requests between the Customer's browser and the Service are relayed in encrypted form through the infrastructure of Vercel Inc., which may process them in the USA. Vercel does not store Customer Data. The transfer is based on Vercel's certification under the EU-US Data Privacy Framework (Art. 45 GDPR) and, in addition, on the EU Standard Contractual Clauses (Art. 46(2)(c) GDPR).

- 8.3 Sovaro transfers Customer Data to other third countries only if the requirements of Art. 44 to 49 GDPR are met.

9. Assistance to the Customer

- 9.1 In line with the nature of the processing, Sovaro assists the Customer with appropriate technical and organisational measures in responding to requests from data subjects exercising their rights under Chapter III GDPR. Because Customer Data is deleted within minutes and is not linked to any user profile, Sovaro will in most cases hold no data to which such a request could relate. Sovaro forwards any request it receives directly from a data subject to the Customer without undue delay.
- 9.2 Sovaro assists the Customer, based on the information available to it, in meeting its obligations under Art. 32 to 36 GDPR (security, breach notifications, data protection impact assessments and prior consultation).

10. Personal data breaches

- 10.1 Sovaro notifies the Customer without undue delay after becoming aware of a personal data breach affecting Customer Data, so that the Customer can meet its own notification obligations within 72 hours.
- 10.2 The notification contains, as far as available, a description of the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken or proposed. Information that is not yet available is provided as soon as it is.
- 10.3 Sovaro takes the measures necessary to contain the breach and mitigate its possible adverse effects, and documents the breach.

11. Deletion and return

- 11.1 Customer Data is deleted automatically after processing and download, and at the latest 15 minutes after processing. The Customer returns the data to itself by downloading the results; after deletion, neither return nor recovery is possible.
- 11.2 At the end of the Agreement, Sovaro therefore holds no Customer Data. Should any Customer Data nevertheless remain, Sovaro deletes it without undue delay, unless Union or Member State law requires its storage.

12. Information and audits

- 12.1 Sovaro makes available to the Customer, on request, all information necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR.

- 12.2** For the infrastructure provided by Amazon Web Services, the Customer may rely on the ISO/IEC 27001 certification, the BSI C5 attestation and the SOC 2 reports of AWS, which Amazon Web Services makes available through AWS Artifact.
- 12.3** The Customer, or an independent auditor bound to confidentiality and appointed by it, may audit Sovaro's compliance with this DPA, in principle once per calendar year and additionally after a personal data breach. Audits must be announced at least 30 days in advance, take place during normal business hours and must not unreasonably disrupt Sovaro's operations. Each party bears its own costs.

13. Liability

- 13.1** Liability towards data subjects is governed by Art. 82 GDPR. In the relationship between the parties, the liability provisions of the Agreement apply.

14. Final provisions

- 14.1** This DPA forms an integral part of the Agreement. In the event of a conflict concerning the protection of personal data, this DPA takes precedence over the other provisions of the Agreement.
- 14.2** Sovaro may amend this DPA where this is necessary because of changes in Data Protection Law, in the guidance of supervisory authorities or in the Service, provided the level of protection is not reduced. Section 14 of the General Terms and Conditions applies to the procedure.
- 14.3** This DPA is governed by Austrian law. The place of jurisdiction follows the Agreement.
- 14.4** Should any provision of this DPA be invalid, the remaining provisions remain valid.

Annex 1: Details of processing

Subject matter	Lossless compression of files submitted by the Customer (PDF, Word, Excel, PowerPoint, PNG, JPEG) and verification of the results against the originals.
Nature of processing	Upload of the files, temporary holding during processing, compression using Sovaro's software and Claude language models provided through Amazon Bedrock, comparison of each result with its original, provision of the results for download (individually or as a ZIP archive) and automatic deletion no later than 15 minutes after processing.
Purpose	Reducing the file size of the Customer's documents, typically before they are uploaded to a virtual data room.

Duration	For each file: from upload until deletion after processing and download, at the latest 15 minutes after processing. Overall: the term of the Agreement.
Types of personal data	Any personal data contained in the submitted files, as determined solely by the Customer, for example names, contact details, job titles, employment, contract, financial and transaction data. File names and the technical data needed to process the request (IP address, file size and type) for the duration of the processing.
Special categories of data	The files may contain special categories of personal data (Art. 9 GDPR) or data relating to criminal convictions (Art. 10 GDPR) if the Customer submits such files. The Customer decides this; the measures in Annex 3 apply to all files alike.
Categories of data subjects	Persons whose data appear in the submitted files, for example employees, managers, shareholders, customers, suppliers and other business partners of the Customer, of its clients or of companies involved in a transaction.
Location of processing	Amazon Web Services, region Europe (Frankfurt), eu-central-1, Germany. Encrypted relay of requests through Vercel as described in section 8.2.

Annex 2: Subprocessors

Subprocessor	Service	Location	Transfer safeguard
Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxembourg	Amazon Web Services (AWS), including Amazon Bedrock: operation of the PreVDR compression service and of the Claude language models it uses; transient processing of Customer Data	AWS Region Europe (Frankfurt), eu-central-1, Germany	Processing in the EU; AWS GDPR Data Processing Addendum
Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, USA	Hosting of the website www.prevdr.com and encrypted relay of requests between the browser and the PreVDR service; no storage of Customer Data	USA and Vercel's global edge network	EU-US Data Privacy Framework and EU Standard Contractual Clauses
IONOS SE, Elgendorfer Str. 57, 56410 Montabaur, Germany	Email hosting for office@prevdr.com; only relevant if the Customer sends files or personal data to Sovaro by email, for example in a support request	Germany	Processing in the EU

Annex 3: Technical and organisational measures

The technical and organisational measures that Sovaro implements under Art. 32 GDPR are described in the document "Technical and organisational measures" (www.prevdr.com/legal/toms) in the version valid at the time. That document forms part of this DPA.