Data Processing Agreement, Rencore Governance, 04/2026

1 Terms and definitions

1.1 Definitions of the GDPR and the Software-as-a-Service Agreement

For the purposes of this Data Processing Addendum, the definitions of Article 4 GDPR apply, unless otherwise defined below in Section 1.2 of this DPA.

1.2 Specific definitions of this Data Processing Addendum

For the purposes of this Data Processing Addendum, the following deviating and/or additional definitions apply:

1.2.1 **"Data Processing Addendum"** or **"DPA"** means this agreement including its Annexes.

1.2.2 **"EEA"** means the European Economic Area.

1.2.3 **"EU"** or **"Union"** means the European Union.

1.2.4 **"Member State"** means a member state of the EU and/or a contracting state of the EEA.

1.2.5 **"General Data Protection Regulation"** or **"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

1.2.6 **"Standard Contractual Clauses"** or **"SCC"** means the standard contractual clauses for the transfer of personal data to third countries annexed to Commission Implementing Decision (EU) 2021/914 as of 4 June 2021.

1.2.7 **"Sub-processor"** means any other processor engaged by a processor pursuant to Article 28 (2) and (4) GDPR.

1.2.8 **"Third Country"** means any country outside the EEA.

2 Scope of applicability, Parties and their respective roles

2.1 Scope of applicability

This DPA applies to any processing of personal data by Rencore in the provision of the Services.

2.2 Parties and their respective roles

For purposes of this DPA, Customer is the controller and Rencore is the processor. Where Customer only acts as a processor for personal data covered by this DPA for another controller, Rencore is a Sub-processor.

3 Details of the processing

The subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects are set out in **Annex 2** to this DPA.

4 Obligations and rights of Customer

4.1 Responsibility of Customer

Customer is responsible for compliance with the obligations applicable to a controller pursuant to the GDPR, in particular compliance with the principles relating to processing of personal data laid down in Chapter II GDPR and compliance with data subjects' rights laid down in Chapter III GDPR.

4.2 Right to issue instructions

4.2.1 Customer has the right to issue instructions to Rencore regarding the processing of personal data under this DPA. Customer shall issue its instructions via email to privacy@rencore.com or in writing to Rencore's registered address, with the understanding that postal instructions are received within 3 business days. To ensure a swift response, Rencore encourages the Customer to communicate with them via the listed email address.

4.2.2 In urgent cases, Customer shall be allowed to issue individual instructions orally. Customer shall confirm oral instructions via email to privacy@rencore.com or in writing without undue delay, with the understanding that postal instructions are received within 3 business days. To ensure a swift response, Rencore encourages the Customer to communicate with them via the listed email address.

4.2.3 Customer shall bear any additional costs and expenses arising for Rencore due to instructions of Customer which deviate from or create additional requirements to the provisions of the Agreement or this DPA.

4.2.4 Rencore shall inform the Customer immediately if, in its opinion, an instruction issued by the Customer violates legal regulations. Rencore is authorised to suspend the implementation of the instruction in question until it is confirmed or amended by the Customer.

4.3 Right to request information and conduct audits, including inspections

4.3.1 Customer has the right to request from Rencore all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and to conduct audits, including inspections, of Rencore by itself or by another auditor mandated by Customer.

4.3.2 Customer shall give Rencore reasonable advance notice before conducting an audit or an inspection. Customer shall carry out inspections during normal business hours. Entry to Rencore's premises shall take place solely in the constant presence of a representative of Rencore. Rencore hereby notifies the Customer that it stores no operative data on premises; Rencore can instead assist the Customer in organizing audits of the relevant Microsoft Azure data centers, where possible. In conducting these audits/inspections, Rencore will restrict access to data that belongs to other customers.

4.3.3 The inspections may be carried out by an independent auditor who is bound to secrecy. The auditor shall send a copy of the audit report to the Rencore at the same time as to the Customer. If costs are incurred for carrying out the audit, these

shall be borne by the Customer. All information disclosed to Customer in connection with the exercise of its rights under Section 4.3.1 of this DPA shall be deemed as Confidential Information.

5 Obligations of Rencore

5.1 Processing on documented instructions from Customer

5.1.1 Rencore processes the personal data which is subject to this DPA only on documented instructions from Customer, including with regard to transfers of personal data to a Third Country or an international organization, unless required to do so by Union or Member State law to which Rencore is subject; in such a case, Rencore shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

5.1.2 Rencore shall be allowed to process anonymized information for its own purposes. For the avoidance of doubt, anonymized data cannot be traced back to an identifiable person by any means.

5.2 Confidentiality of persons authorized to process the personal data

Rencore ensures that persons authorized to process the personal data which is subject to this DPA have committed themselves to confidentiality.

5.3 Security of the processing

5.3.1 Rencore shall take all measures required pursuant to Article 32 GDPR.

5.3.2 The specific measures to be taken by Rencore are set out in **Annex 3** to this DPA.

5.3.3 The technical and organizational measures are subject to technological progress and refinement. Rencore is therefore entitled to take additional or alternative measures to the measures set out in **Annex 3** to this DPA, as long as this does not result in a decrease in the security level of the technical and organizational measures in place at Rencore. Rencore shall document amendments to the measures and provide this documentation to Customer upon the Customer's request.

5.3.4 Rencore shall notify Customer without undue delay after becoming aware of a personal data breach relating to personal data which is subject to this DPA.

5.4 Engagement of another processor (Sub-processor)

5.4.1 Rencore respects the following conditions referred to in Article 28 (2) and (4) GDPR for engaging another processor:

5.4.1.1 Rencore shall not engage another processor without authorization of Customer. This means that Rencore shall inform Customer at least four weeks in advance of any intended changes concerning the addition or replacement of other processors (email being sufficient), thereby giving Customer the opportunity to object to such changes within 14 days following the information by notifying Rencore of such objection.

5.4.1.2 In case of objections, Rencore shall use commercially reasonable efforts to provide Customer with a change to Rencore's products and/or services or recommend a commercially reasonable change to Rencore's configuration or use of Rencore's products and/or services in order to avoid the processing of personal data by the objected-to new sub-processor without unduly burdening Customer. If Rencore is not able to make such changes, either party may terminate the SaaS Agreement extraordinarily and without notice without forfeiting any contractual penalty. Rencore shall reimburse the Customer for any fees paid in advance on a pro rata basis.

5.4.1.3 Where Rencore engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in this DPA shall be imposed on that other processor by way of a contract, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR.

5.4.1.4 Where that other processor fails to fulfil its data protection obligations, Rencore shall remain fully liable to the Customer for the performance of that other processor's obligations.

5.4.2 Customer hereby grants the specific authorization to the engagement of the Sub-processors set out in the current list available at [link] and further grants the general authorization to the engagement of Sub-processors under the conditions laid down in Section 5.4.1 of this DPA.

5.5 Assistance for the fulfilment of Customer's obligation to respond to requests for exercising the data subject's rights

Rencore, taking into account the nature of the processing, assists Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR relating to personal data which is subject to this DPA.

5.6 Assistance in ensuring Customer's compliance with the obligations regarding security of the processing, the documentation, notification and communication of personal data breaches, completion of data protection impact assessment and prior notification

Rencore assists Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to Rencore relating to personal data which is subject to this DPA.

5.7 Deletion or return of the personal data to Customer after the end of the provision of Services

Rencore, at the choice of Customer, deletes or returns all the personal data which is subject to this DPA to Customer after the end of the provision of the Services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data. Data may be held for a longer period where this is required for backup purposes (as part of having adequate technical and organizational measures), for legal reasons, or to allow for a restoration of services in the event of accidental deletion. In the first two instances, data will only be stored for

the period which is it required to fulfil these purposes; in the third instance, data will be queued for deletion for 30 days before it is permanently deleted.

In the event that Customer's Rencore Governance subscription lapses, associated workspaces will be archived for 30 days and then the data will be queued for deletion for an additional 30 days, meaning that the workspace data will be permanently deleted 60 days after the subscription expires.

6 Transfers of personal data to Third Countries

6.1 **Rencore will not transfer personal data** to Third Countries without a sufficient basis for doing so under Chapter V GDPR.

6.2 All transfers to Sub-processors based outside of the EEA or otherwise communicated to the Customer are based on appropriate safeguarding mechanisms in combination with strict technical, organizational and contractual measures, as referenced in **Annex 3**. Rencore will provide information on these standard contractual clauses on request. Should a Sub-processor outside of the EEA receive data on the basis of another justification under Chapter V GDPR, this alternative justification will be listed.

7 Term and termination

This Data Processing Addendum comes into force upon commencement of Services in accordance with date listed on the Order Form. The term of this DPA is subject to the deletion of Customer personal data after termination of the Agreement.

8 Final provisions

8.1 Amendments and additions to this Data Processing Addendum

Amendments and additions to this DPA require the written form. This also applies to any waiver of the written form requirement. The written form may be substituted by the electronic form, which is taken to include in-product prompts and checkboxes, unless stated otherwise in this Agreement or any amendment to this Agreement.

8.2 Severability

If any provision of this Data Processing Addendum is or becomes fully or partly invalid or unenforceable, this shall not affect the validity of the remaining provisions. The Parties undertake to jointly replace the invalid or unenforceable provision with a valid provision which comes as close as possible to the invalid or unenforceable one. The same applies to any omission in this DPA.

8.3 Order of precedence

In case of conflicts between this DPA and other agreements between the Parties, the provisions of this DPA shall prevail.

8.4 Applicable Law

The laws of the Federal Republic of Germany shall apply to the DPA.

Annexes:

Annex 1 – List of parties

Annex 2 – Description of the processing

Annex 3 – Security measures

Annex 1 – List of parties

Controller

Name: As listed on the Order form for Services

Address: As listed on the Order Form for Services

Contact person's name, position and contact details: As listed on the Order Form for Services

Processor

Name: Rencore GmbH

Address: Rencore GmbH, Bayerstrasse 71-73, 80335 Munich, Germany

Contact person's name, position and contact details: Charlotte Cutts, Data Protection & Compliance Officer, privacy@rencore.com (above postal address can be used, but notices will be processed quicker if sent to the listed email address)

A signed version of this Data Processing Agreement is available here [link]. A mutual signing process can be set up on request.

Annex 2 – Description of the processing

Categories of data subjects whose personal data is processed:

Any category of person that the Customer gives an account in their instance of M365, or whose details otherwise appear in M365 metadata, e.g. file names. This is in the sole determination of the Customer. In the typical use of Rencore Governance, at least some Customer employees will be data subjects for the purpose of this DPA.

Categories of personal data processed:

All plausible user profile metadata within M365, where this metadata contains personal data (e.g. usernames, job descriptions). Also some file metadata (file names, date modified, who modified). Under no circumstances is personal data in the contents of files processed by Rencore Governance. See here for a comprehensive inventory of elements that may be processed in Rencore Governance: https://url.rencore.com/gov-inventory

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved:

Ordinary use of Rencore Governance does not result in the processing of sensitive data in accordance with Art. 8-10 GDPR. In the event that a Customer chooses to include this data in Microsoft 365 metadata, which is not considered standard use of Rencore Governance, this data would be protected by the technical and organisational measures listed in **Annex 3**.

Nature of the processing:

Note: all processing activities within Rencore Governance are actioned by the Customer themselves through using the tool; **neither employees/contractors etc. of Rencore GmbH nor the tool of its own accord processes any personal data without being instructed or directed by the Customer.**

Rencore Governance **collects** and **records** metadata in real time gathered from a connected instance of M365, including any personal data that appears in this metadata (see the following link for an inventory of all potential interactions of Rencore Governance with personal data: https://url.rencore.com/gov-inventory). It also processes standard user account data of registered Rencore Governance users.

Rencore Governance may **organize** and **structure** data within M365 if the Customer opts into workflows that allow for Rencore Governance to carry out these specific processing activities.

Any data that Rencore Governance processes (including personal data that appears as metadata) will be **stored** in a Microsoft Azure data center selected by the Customer. Microsoft acts in this capacity as a Sub-processor acting on behalf of Rencore GmbH. This pertains purely to the metadata referenced above – Rencore does not make a copy of all data in the Customer's M365 instance, and the Customer retains control and responsibility over where their M365 data is stored.

Rencore Governance can **adapt** or **alter** the listed metadata within M365 if the Customer opts into workflows that allow for Rencore Governance to carry out these specific processing activities.

Rencore Governance may be used to **retrieve** metadata in a M365 instance. Rencore Governance may carry out some automated **analyses**, which could include personal data that features in the Customer's relevant metadata. This would not amount to automated decision-making and/or profiling in accordance with Art. 22 GDPR unless the Customer of its own accord decides to set up such a system using Rencore Governance, against Rencore's advice.

Rencore Governance could theoretically be used to assist in finding data in order to **disclose** it with lawful reason to others, e.g. to assist in a Customer's obligation to respond to requests to exercise the data subject rights set out in Chapter III of the GDPR (Section 5.5 of this DPA). However, this is not the primary goal of the tool, especially since the tool only processes metadata.

In conducting its scans, Rencore Governance often compares old datasets in Rencore Governance with new datasets found in the Customer's M365 tenant, in doing so carrying out an **alignment** of the data and updating the old dataset in Rencore Governance. The extent to which this occurs depends on the workflows that the Customer allows to run in Rencore Governance and depends on the scan frequency and the amount of data to be scanned.

Rencore Governance may **combine** personal data in order to generate dashboard overviews of data; the extent of this depends on how the Customer has set up these dashboards.

Rencore Governance may **restrict** access to the listed metadata within M365 if the Customer opts into workflows that allow for Rencore Governance to carry out these specific processing activities.

Purpose(s) for which the personal data is processed on behalf of the controller:

The processing serves the purpose of provision of the Services outlined in the Order Form.

Duration of the processing:

The duration of the processing is determined by the duration of the provision of the Services plus any deletion periods data is subject to after the termination of Services.

The above description refers to processing carried out by Rencore GmbH during the provision of Rencore Governance Services: a full list of Sub-processors and analogous details of their processing activities is available here [link].

Annex 3 – Security measures

1. Pseudonymization of personal data (Article 32 (1) (a) GDPR)

Rencore Governance does not generally pseudonymize personal data, because this is at odds with the purpose of the product (to manage metadata within M365 so that use of M365 can be optimized). There are some minor instances in which data in M365 can be pseudonymized (https://url.rencore.com/un-anonymize), and the Customer themselves can deploy their own system of pseudonymization if they wish, e.g. using a string of letters and numbers for usernames within M365 rather than people's full names.

Rencore's practices regarding the deletion and destruction of customer data are detailed in Rencore's Backup Policy, available on request from Rencore's Trust Center (https://trust.rencore.com). When data retention periods have lapsed, data is fully destroyed – it is not kept in a pseudonymized/non-anonymized state for longer periods of time, except in the event of required security backups.

2. Encryption of personal data (Article 32 (1) (a) GDPR)

In Rencore Governance, all information is encrypted: Azure Storage Accounts and PostgreSQL have built-in support for encryption at rest and in-transit. Encryption keys are held securely in Microsoft Azure Key Vault. All transmissions from the application to the end-user are TLS 1.3-encrypted; Rencore also makes use of VPNs where appropriate during the production process and ensures that any physical documentation/data related to business dealings is transported securely.

More information about this is available in Rencore's documentation, available at https://url.rencore.com/security; this link is also informative regarding other security topics.

3. Ability to ensure the ongoing confidentiality of processing systems and services (Article 32 (1) (b) GDPR)

Only authorized personnel have access to production systems where personal data exists or is processed. All authorized personnel sign a confidentiality agreement that covers all Customer data.

4. Ability to ensure the ongoing integrity of processing systems and services (Article 32 (1) (b) GDPR)

Audit logs are kept for Rencore systems, including access to processing and cloud environments. Duration of storage of log files depends on the type of log:

- Customer logs are kept for a year;
- Non-product generated security logs are kept for 18 months, including Rencore's own activities against Azure resources. These are fed into Azure Sentinel. This includes Front Door access and firewall logs;
- At least 90 days of product-generated logs are stored in the regional Log Analytics workspaces;

- Application Insights logs are kept for 90 days.

Only authorized personnel at Rencore can access the audit logs; such access is provided on a need-to-know basis. All systems are configured according to security best practices. Customers are either given access to the contents of these logs through self-service mechanisms or are entitled to see the contents of these logs, unless the contents of these logs reveal confidential information about Rencore's internal operations and/or the internal operations of other customers.

5. Ability to ensure the ongoing availability of processing systems and services (Article 32 (1) (b) GDPR)

Rencore Governance makes use of Microsoft Azure data centers to store all of its data, which are adequately redundant in line with their SOC 2 accreditation and ISO 27001 certification (for more information on how Microsoft Azure data centers are set up to ensure ongoing availability, please refer to the following resource: https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy) and have the required protections against physical compromise and cyberattacks (refer to the following resource for further information on Microsoft Azure's security measures: https://docs.microsoft.com/en-us/azure/security/fundamentals/overview). Rencore uses a locally redundant storage model with regard to these data centers. Rencore has an analogous level of security, including the use of firewalls. All systems are configured to be available during high load.

6. Ability to ensure the ongoing resilience of processing systems and services (Article 32 (1) (b) GDPR)

All systems are built as resilient, cloud-native applications and adopt security best practices; Rencore Governance is designed and architected from Microsoft best practices for distributed cloud solutions. The system scales up as high demand arises, and all applications run multiple instances to distribute and load-balance the incoming requests.

7. Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident (Article 32 (1) (c) GDPR)

We adhere to our Rencore Backup Policy for data backups (this can be found in Rencore's Trust Center: https://trust.rencore.com). Rencore Governance has regular backups of configurations, and the infrastructure can be replicated in the same or new regions, in the event of a technical incident.

Rencore Governance operates in Microsoft Azure, and as such, is dependent on services from Microsoft Azure. If an incident is because of service degradation of Microsoft Azure, Rencore may be impacted by this, but Microsoft is well-placed to respond to such incidents (please refer to the aforementioned resources regarding redundancies).

8. Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing (Article 32 (1) (d) GDPR)

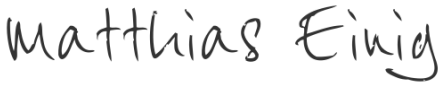
Rencore has a SOC 2 accreditation and an ISO 27001/ISO 27017 certification, which are subject to annual external audits. Reviews of technical and organizational measures occur on a regular basis, at the very least once per year but more frequently if the need arises.

9. Other measures (Article 32 (1) GDPR)

Please refer to the additional security documentation provided by Rencore in its Trust Center (https://trust.rencore.com/) for a comprehensive overview of all technical, organizational and administrative measures put in place by Rencore.

Record of Signing

For	Rencore
Name	Matthias Einig
Title	CEO



Signed on Apr 10, 2026 6:01 PM CEST

Secured by Concord™
DocumentID: 032xGlFTeSUUU29rnkMGu3
SigningID: 032xGlFTMKLlrDJtxFWa7R
UTC Signing time: 2026-04-10 16:01:28 UTC
IP Address: 153.100.179.232
Email: matthias.einig@rencore.com