Annex 2 – Data Processing Addendum for the Software-as-a-Service Agreement

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 and of Clause 1.1 of the Software-as-a-Service Agreement 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 Schedules.

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 **Schedule 1** 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.

4.3   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 notify Rencore in due time, at least two (2) weeks in advance, before conducting an audit, including 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 organising audits of the relevant Microsoft Azure data centres, where possible. In conducting these audits/inspections, Rencore will restrict access to data that belongs to other customers.

4.3.3   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.

4.3.4   Customer shall bear its own costs of audits, including inspections, and the costs reasonably arising thereby for Rencore unless any defects found during the audit are based on a culpable breach by Rencore against this DPA or instructions of Customer.

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 organisation, 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 anonymised information for its own purposes. For the avoidance of doubt, anonymised data cannot be traced back to an identifiable person by any means.

5.2 Confidentiality of persons authorised to process the personal data

Rencore ensures that persons authorised 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 **Schedule 2** to this DPA.

5.3.3 The technical and organisational measures are subject to technological progress and refinement. Rencore is therefore entitled to take additional or alternative measures to the measures set out in **Schedule 2** to this DPA, as long as this does not result in a decrease in the security level of the technical and organisational 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 general written authorisation 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.

5.4.1.2 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 organisational measures in such a manner that the processing will meet the requirements of the GDPR.

5.4.1.3 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 authorisation to the engagement of the Sub-processors set out in **Schedule 3** and further grants the general authorisation 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 organisational 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 organisational 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.

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 listed in Schedule 3 or otherwise communicated to the Customer are based on standard contractual clauses in combination with strict technical, organisational and contractual measures, as referenced in Schedule 2. Rencore will provide information on these standard contractual clauses on request. Should a Sub-processor in the EEA receive data on the basis of

another justification under Chapter V GDPR, this alternative justification will be listed in Schedule 3.

7   Term and termination

This Data Processing Addendum comes into force upon signature of the Agreement by the Parties. The term of this DPA corresponds to the term 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 (*Schriftform*). 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.

<u>Schedules:</u>

Schedule 1 – Details of the processing

Schedule 2 – Security measures

Schedule 3 – Sub-processors

Schedule 1 – Details of the processing

1.   **Subject-matter of the processing**

> The subject matter of the processing is the provision of the Services outlined in the Software-as-a-Service Agreement.

2.   **Duration of the processing**

> The duration of the processing is determined by the duration of the provision of the Services outlined in the Software-as-a-Service Agreement, unless otherwise specified in other parts of this DPA.

3.   **Purpose of the processing**

> The processing serves the purpose of provision of the Services outlined in the Software-as-a-Service Agreement.
>
> Insofar as Rencore processes personal data in order to assist Customer in fulfilling its 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), the processing also serves the purpose of fulfilling the legal obligations of the controller under Chapter III of the GDPR.
>
> Insofar as Rencore processes personal data in order to assist Customer in fulfilling the obligations set out in Articles 32 to 36 of the GDPR (Section 5.6 of this DPA), the processing shall also serve the purpose of fulfilling the legal obligations of the controller under Articles 32 to 36 of the GDPR.

4.   **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.** This is to be taken into consideration with regard to the answers given below. Rencore Governance has read-only access to the M365 tenant, unless the Customer opts into specific workflows that allow Rencore Governance to edit information in Microsoft 365.

☒	Collection, recording:	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.
☒	Organisation, structuring:	Rencore Governance can only reorganise and restructure data within M365 if the Customer opts into workflows that allow for Rencore Governance to carry out

		these specific processing activities; if the Customer does not opt into these workflows, Rencore Governance scans the M365 tenant of the Customer and can only flag where (re)organisation or (re)structuring is advisable.
☒	Storage:	Any data that Rencore Governance processes (including personal data that appears as metadata) will be stored at a Microsoft Azure data centre 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.
☒	Adaption, alteration:	Rencore Governance can only 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; if the Customer does not opt into these workflows, Rencore Governance scans the M365 tenant of the Customer and can only flag where adaptions or alterations are advisable.
☒	Retrieval, consultation:	Rencore Governance may be used to retrieve metadata, including metadata that is dormant, in a M365 instance. This could in theory be useful in responding to requests to exercise the data subject rights set out in Chapter III of the GDPR (see section 5.5 of this DPA), with regard to retrieving data; however, Rencore Governance is not primarily designed to act as a comprehensive e-discovery service. Rencore Governance does not carry out any form of "consulting" activity with regard to this data except for 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.
☐	Use:	Rencore is a data management tool; it does not make use of the data itself, except for "use" in a broader sense that comprises all other processing activities indicated in this table.
☒	Disclosure (by transmission, dissemination or otherwise making available):	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.

		Rencore Governance otherwise only transmits data to others in line with **Schedule 3** of this DPA, with regard to data transmission to Sub-processors.
☒	Alignment:	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.
☒	Combination:	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.
☒	Restriction:	Rencore Governance can only 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. If the Customer does not opt into these workflows, Rencore Governance scans the M365 tenant of the Customer and can only flag where restrictions are advisable.
☐	Erasure, destruction:	Regardless of which workflows are activated in Rencore Governance, at most, data can only be moved into the Microsoft SharePoint recycling bin, which is emptied automatically after a set period of time. Permanent deletion is only possible directly within the M365 tenant and therefore outside of Rencore Governance, and this must be actioned directly by the Customer. The data that Rencore GmbH itself holds (a copy of metadata) is erased at the choice of Customer after the end of the provision of the Services relating to processing (Section 5.7 of this DPA), or transferred back to the Customer at their request. The Customer can delete, or request deletion of, scan data at any time.
☒	Others:	Should the Customer run into issues while using Rencore Governance, the Customer is able to file a support ticket. Personal data may be processed through interacting with the internal support team in order to resolve the issue (Rencore does not make use of an external support team; all support team members are employees of Rencore who have signed an appropriate NDA). Personal data may also be processed with regard to charging for the Rencore Governance subscription, providing feedback on Rencore Governance, using the inbuilt user guide tool, using the internal messaging functions of

		Rencore Governance or to identify patterns of user behaviour within Rencore Governance for the purpose of improving the product. This is detailed further under **Schedule 3**, regarding the table of subprocessors.

5.   Type of personal data

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). This is highly unlikely to include any data that is relevant to Art. 8-10 GDPR (sensitive personal data); the inclusion of any such personal data is in the sole determination of the Customer as controller of this data. 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

Where a ticket is opened with Rencore's support team, personal data may be processed where necessary to correctly respond to the ticket, i.e. name, email address, further contact details. Rencore support does not carry out remote desktop access or participate in video calls with the Customer, unless this is requested by the Customer and therefore with their consent. The processing of tickets may require screenshots of errors to be sent, which could capture personal data depending on how the Customer takes the screenshots. The user metadata within M365 and other PII within Rencore Governance itself, as listed above, may be accessed by those with access to Rencore Governance's administrator portal for the purposes of providing support (select members of the Customer Success, Product Management and Product Operations department, as controlled and determined through strict access control policies – please refer to Rencore's System Access Control Policy, which is available in Rencore's Trust Center: https://trust.rencore.com).

Personal data may be processed with regard to setting up user accounts for Rencore Governance (i.e. standard user account information, such as username and email address), and with regard to making payment for the Rencore Governance subscription, i.e. name and email address of the Customer employee responsible for making the payment. In the course of using the direct and indirect feedback tools (Userback and Pendo) and the user guide tool for Rencore Governance, IP address and user behaviour data may be processed, with regard to using these tools. The internal messaging feature will process any personal data within the contents of these messages and also information required to send/receive the messages, e.g. email addresses.

6.   Categories of data subjects

☒	Customer's employees

☒	Customer's job applicants (only in the event that people in this category use the Customer's M365 tenant or are otherwise referenced in M365 metadata)
☒	Customer's customers and their employees (only in the event that people in this category use the Customer's M365 tenant, are otherwise referenced in M365 metadata or use Support-Services)
☒	Customer's prospect customers and their employees (only in the event that people in this category use the Customer's M365 tenant, are otherwise referenced in M365 metadata or use Support-Services)
☒	Customer's suppliers and their employees (only in the event that people in this category use the Customer's M365 tenant, are otherwise referenced in M365 metadata or use Support-Services)
☒	Customer's visitors (only in the event that people in this category use the Customer's M365 tenant or are otherwise referenced in M365 metadata)
☒	Users of Customer's websites/apps (only in the event that people in this category use the Customer's M365 tenant or are otherwise referenced in M365 metadata)
☒	Others:	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.

Schedule 2 – Security measures

Please refer additionally to Rencore's separate TOMs overview, which can be provided on request.

1. **Pseudonymisation of personal data (Article 32 (1) (a) GDPR)**

   Rencore Governance does not generally pseudonymise 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 optimised). There are some minor instances in which data in M365 can be pseudonymised (https://url.rencore.com/un-anonymize), and the Customer themselves can deploy their own system of pseudonymisation if they wish, e.g. using a string of letters and numbers for usernames within M365 rather than people's full names.

   Permanent deletion of data out of Rencore Governance always comprises a full destruction of the data that renders it anonymous in the process. The same applies to Rencore's practices regarding the deletion and destruction of business data.

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. In addition to this, Rencore Governance adds another layer of cryptographic AES 256-bit industry-standard encryption around the data before it is transmitted to the storage; this encryption key is held securely in Microsoft Azure Key Vault. All transmissions from the application to the end-user are SSL 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 depend on the type of log:

   - Customer logs are kept for a year;

   - Product generated logs are kept available for 2 months;

- Security-related logs are kept for 18 months.

Only authorised 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.

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 centres 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 centres 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 MS Azure's security measures: https://docs.microsoft.com/en-us/azure/security/fundamentals/overview). 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 with Microsoft Azure, Rencore might 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 organisational measures for ensuring the security of the processing (Article 32 (1) (d) GDPR)**

Rencore has a SOC 2 accreditation, which is renewed annually. Rencore is also working towards meeting the requirements of ISO 27001 over a longer period of time.

Reviews of technical and organisational 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 TOMs overview (provided on request) and additional security documentation provided by Rencore in its Trust Center (https://trust.rencore.com/) for a comprehensive overview of all technical, organisational and administrative measures put in place by Rencore.

Schedule 3 – Sub-processors

All transfers of personal data outside of the EEA are performed on the basis of Art. 46 (2) (c) GDPR (application of the newest standard contractual clauses), with the exception of transfers to the US resulting from interactions with Microsoft and HubSpot: these companies are both on the EU-US Data Privacy Framework List.

Name and address of Sub-processor	Scope, nature and purpose of Sub-processing	Categories of data subjects	Types of personal data	Duration of Sub-processing	Location of the Sub-processing
Microsoft (Azure/Application Insights)	Azure: cloud storage for Rencore Governance and associated scan data/app hosting Application Insights: logging and processing of error data to assist in error resolution	The Customer's M365 users/those whose PII is referenced in the M365 tenant; Rencore Governance user	Azure: User profile data in Rencore Governance/M365; metadata generated by the use of M365 Application Insights: user IDs, exception details of external libraries and APIs, IP address, city, region	Duration of Rencore Governance subscription, with a 30-day hold before permanent deletion; Application Insight logs are kept for 3 months after they are generated, regardless of end of subscription	Microsoft Germany West Central data centre, as long as selected by Customer on connection of Rencore Governance with the M365 tenant – other options are Central US and Australia East
HubSpot (integration can be deactivated)	Operation of chat icon/support chat system within Rencore Governance; CRM system integration	The Customer's M365 users/those whose PII is referenced in the M365 tenant, where relevant to the ticket;	User IDs, chat communications, chat metadata, subscription data in CRM system	Duration of Rencore Governance subscription, longer where necessary for legal/accounting purposes or for the purposes of future troubleshooting	United States (in the process of being moved to HubSpot's new EU data centre)

Software-as-a-Service Agreement for Rencore Governance, v.1.2 (as of August 2024) Concord · Document ID: 0e9c6a2fa06b000bZK3mLubm7ba2C   14-17

Page 14/17

		Rencore Governance user			
Chargebee	Rencore Governance subscription management	Customer/any assigned payers of the Customer, e.g. assigned member of Customer's procurement department	Email address, username	Duration of Rencore Governance subscription, longer where necessary for legal/accounting purposes; should Rencore in the future decide to no longer work with Chargebee, Chargebee will retain data for 120 days before permanently deleting it.	Germany
Sendgrid (integration can be deactivated, with the exception of user invitation emails)	Messaging service operating within Rencore Governance – this function can be carried out by an SMTP server or Microsoft 365 instead of Sendgrid in all cases except for inviting users to workspace, since those messages originate from Rencore's system	The Customer's M365 users; Rencore Governance users	Email address, internal message contents	Duration of Rencore Governance subscription. Sent messages may be stored for longer in end-user email clients	United States (storage in an Amazon Web Services data centre)
Userback (integration can be deactivated)	Allows Customer to share feedback with Rencore	Rencore Governance users	Email address; name; text feedback, screenshots and video recordings (feedback may or may not contain PII - this is context dependent); session information (browser version, screen settings, OS, associated workspace, name of page loaded, date and time)	Until no longer serves purpose of collection – feedback is given under the understanding that Rencore can continue to use it post-subscription	United States (storage in an Amazon Web Services data centre)

| Pendo (integration can be deactivated) | Collection of information on use of Rencore Governance to allow continual improvement of users' experience: Rencore creates dashboards, KPIs and metrics out of this information to help product development. Information may also be used in troubleshooting efforts.

To create guided user journeys based on behavioural segmentation. | Rencore Governance users | Unique identifier of Rencore Governance users (not M365 users) - unique identifier can be used to derive name, company and company email address; Workspace/Environment information (ID, name); timeline for usage per Rencore Governance user; Pages visited; Features used; Events encountered (errors, exceptions, etc.); Poll responses; Product Guides watched; OS/browser/device information | Until no longer serves purpose of collection (product improvement, troubleshooting) | European Union |

For	Rencore
Name	Matthias Einig
Title	CEO

Matthias Einig

Signed on 2024-08-19 15:36:00 GMT

Secured by Concord™
DocumentID: 02xRq3ReCZK3mLubm7ba2C
SigningID: 02xRq3Re0Tte6FQApc6G2n
Signing date: 8/19/2024
IP Address: 153.100.179.115
Email: matthias.einig@rencore.com

concord™
Where agreements happen.