Rencore Governance - Data Protection Agreement

(Controller to Processor)

This Data Processing Agreement ("**DPA**") is entered into by and between:

(i) (Customer) with its registered office at (Address) ("**Controller**"); and

(ii) Rencore GmbH with its registered office at Bayerstrasse 71-73 80335 Munich, Germany (**"Contractor or Processor**"),

each a "**Party**", together the "**Parties**".

1 PREAMBLE

WHEREAS, under the Data Processing Agreement ("**Agreement**") concluded between Processor and Controller, Processor agreed to provide certain services relating to **Rencore Governance** to the Controller as further specified in the Agreement and in Annex 1 to this DPA (the "**Services**");

WHEREAS, in rendering the Services, Processor may from time to time be provided with, or have access to information which may qualify as personal data within the meaning of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**"), and other applicable data protection laws and provisions;

WHEREAS, Controller engages Processor as a commissioned Processor acting on behalf of Controller as stipulated in Art. 28 GDPR;

NOW, **THEREFORE**, and in order to enable the parties to carry out their relationship in a manner that is compliant with law, the parties have entered into this DPA as follows:

2 Terminology

For the purposes of this DPA, the terminology and definitions as used by the GDPR shall apply. In addition to that,

"Member State"	**shall mean a country belonging to the European Union or to the European Economic Area;**
"Subprocessor"	**shall mean any further processor, located within or outside of the EU/EEA, that is engaged by Processor as a sub-contractor for the performance of the Services or parts of the Services on behalf of Controller provided that such Subprocessor has access to the personal data of Controller exclusively for purposes of carrying out the subcontracted Services on behalf of Controller.**
"Security Breach"	**shall mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which affects the personal data of the Controller covered by this DPA.**

Further definitions are provided throughout this DPA.

3 Details of the processing

The details of the processing operations provided by Processor to Controller as a commissioned data processor (e.g., the subject-matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects) are specified in Annex 1 to this DPA.

4 Obligations and responsibilities of Controller

The Controller is responsible that the processing activities relating to the personal data, as specified in the Agreement and this DPA, are lawful, fair and transparent in relation to the data subjects, as set out in Annex 1.

5 Instructions

a) The Processor is obliged to process the personal data only on behalf of the Controller and in accordance with the instructions given by the Controller unless otherwise required by European Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

b) The Controller's instructions are provided in this DPA and the Agreement. Controller may give specifications to such instructions provided in this DPA and the Agreement as well as further instructions. Such specifications and/or further instructions are given generally in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Specifications and/or further instructions in another form than in writing shall be confirmed by Controller in writing without delay. Any further instructions that go beyond the instructions contained in this DPA or the Agreement shall be within the subject matter of the Agreement and this DPA.

c) The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other applicable European Union or Member State data protection provisions ("**Challenged Instruction**"). If the Processor is of the opinion that an instruction infringes the GDPR or other applicable European Union or Member State data

protection provisions, the Processor is not obliged to follow the Challenged Instruction unless and until the Controller has confirmed or changed it.

6 Obligations of Processor

a) The Processor is obliged to ensure that persons authorized by the Processor to process the personal data on behalf of the Controller, in particular the Processor's employees as well as employees of any Subprocessors, have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and that such persons who have access to the personal data process such personal data in compliance with the Controller's instructions.

b) The Processor is obliged to implement the technical and organizational measures as specified in Annex 2 before processing the personal data on behalf of the Controller. The Processor may amend the technical and organizational measures from time to time provided that the amended technical and organizational measures are not less protective as those set out in Annex 2. Substantial amendments to the technical and organizational measures shall be agreed upon in writing between the Parties prior to their implementation. The Processor shall document changes to the technical and organizational measures and provide the Controller with such documentation with being asked.

c) The Processor is obliged to make available to the Controller any information necessary to demonstrate compliance with the obligations of Processor laid down in Art. 28 GDPR and in this DPA. In particular, the Processor will provide an annual audit report based on ISO 27001 or ISAE3402 or SSAE16-SOC 1 Type 2 or ISAE3000 or SSAE16-SOC 2 Type 2 or similar or similar audit reports created by a third party ("Audit Report") as soon as such Audit Report becomes available to Processor.

d) The Processor shall grant Controller or an auditor commissioned by Controller the necessary access, information and inspection rights for this purpose. The Processor undertakes in particular to grant Controller or the auditor appointed by it access to the data processing facilities, files and other documents in order to enable the inspection and verification of the relevant data processing facilities, files and other documentation relating to the processing of Controller's data. The Processor shall provide Controller or the auditor commissioned by Controller with all information necessary for the inspection. The parties agree that access to data of other Rencore clients in the context of an audit must be excluded under all circumstances. The audit right relates exclusively to technical and organisational measures regarding data processing operations concerning Controller.

e) Controller shall be entitled to enter the Processor's business premises where "Principal Data" are processed, with reasonable advance notice during normal business hours (Mondays to Fridays from 9.00 a.m. to 5.00 p.m.) at its own expense, without disrupting the course of business and subject to strict confidentiality of the Processor's business and trade secrets, in order to satisfy itself of compliance with the technical and organisational measures pursuant to Appendix 2 to this Contract. Controller shall pay reasonable compensation for any disruptions to the Processor's operations or for the provision of the Processor's personnel. If the audit demonstrates that The Processor has breached any obligation under this agreement, the Processor shall immediately cure that breach and pay or reimburse Controller for all reasonable costs of the audit. Otherwise Controller shall bear its own costs of the audit.

f) The Processor is obliged to notify the Controller without undue delay
   (i) about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as by a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation; and
   (ii) about any complaints and requests received directly from a data subject (e.g., regarding access, rectification, erasure, restriction of processing, data portability, objection to processing of data, automated decision-making) without responding to that request unless the Processor has been otherwise authorized by the Controller to do so.

g) The processor is obliged to notify the Controller without undue delay about a Security Breach at the Processor or its Subprocessors after the Processor becomes aware of such a Security Breach and in this case the Processor will

assist the Controller with the Controller's obligation under applicable data protection law to inform the data subjects and the supervisory authorities, as applicable, by providing the necessary information taking into account the nature of the processing and the information available to the Processor.

h) The Processor is obliged to assist the Controller with its obligation to carry out a data protection impact assessment as may be required by Art. 35 GDPR and prior consultation as may be required by Art. 36 GDPR that relates to the Services provided by the Processor to the Controller under this DPA by means of providing the necessary and available information to the Controller.

i) The Processor is obliged - at the choice of the Controller - to delete or return to the Controller all the personal data which are processed by the Processor on behalf of the Controller under this DPA after the end of the provision of Services, and delete any existing copies unless European Union or Member State law requires the Processor to retain such personal data.

j) The Processor is obliged to provide to the Controller the respective records of processing activities according to Art. 30 (2) GDPR relating to the Services under this DPA, to the extent necessary for the Controller to comply with its obligation to maintain records of processing.

k) The Processor shall designate a data protection officer and/or a representative, to the extent required by applicable data protection law. The Processor is obliged to provide contact details of the data protection officer and/or representative, if any, to the Controller.

7 Data subject rights

a) The Controller is primarily responsible for handling and responding to requests made by data subjects.

b) The Processor is obliged to assist the Controller with any appropriate and possible technical and organizational measures to respond to requests for exercising the data subjects' rights which are laid down in Chapter III of the GDPR. In particular, the Processor shall assist as follows:

(i) With regard to information requests (Art. 13 and 14 GDPR) the Processor shall provide to the Controller the information as required by Art. 13 and 14 GDPR and as available at the Processor.

(ii) With regard to access requests (Art. 15 GDPR) the Processor shall provide the Controller with the information that needs to be provided to a data subject relating to such an access request and that is available at the Processor.

(iii) With regard to rectification requests (Art. 16 GDPR), erasure requests (Art. 17 GDPR), restriction of processing requests (Art. 18 GDPR), and portability requests (Art. 20 GDPR), the Processor shall either provide the Controller with the ability to rectify or, as the case may be, erase, restrict, or transmit to another third party the affected personal data or if such ability cannot be provided the Processor shall provide the necessary assistance to rectify or, as the case may be, erase, restrict, or transmit to another third party the affected personal data.

(iv) With regard to notification regarding rectification or erasure or restriction of processing (Art. 19 GDPR), the Processor shall assist with notifying any recipients of the personal data that are engaged by the Processor as Subprocessors if requested to do so by the Controller.

(v) With regard to the right to object as exercised by a data subject (Art. 21 and 22 GDPR) the Controller shall determine whether the objection is legitimate and how to address the objection. If the Controller needs the Processor's assistance to address the objection, the Controller shall give a specification to the instructions contained in the DPA as stipulated in Section 5 b) and the Processor will provide such assistance to address the objection.

c) In addition to the assistance specified in 7 b) above, the Controller may request and require additional assistance from the Processor in order to comply with the rights exercised by the data subjects.

d) The Controller is obliged to determine whether or not a data subject has a right to exercise any such data subject rights as set out in this Section 7 and to give specifications to the Processor to what extent the assistance specified in Section 7 b) is required.

8 Subprocessing

a) The Processor shall not engage any Subprocessor without prior written specific authorization of the Controller.

Sub-processors:

Name Sub-processor	**Category of Personal Data**	**Purpose of Processing**	**Country of Processing**
Microsoft	Service context	Services	US, Netherlands or Australia (customer chooses upon creation of account)
HubSpot	User context	Services & Support	US (currently seeking to use HubSpot's new data centre in the EU)
Chargebee	User context	Legal & Contractual	Germany
Sendgrid	User context	Services	US
Userback	User context	Services & Support	US
Userpilot	User context	Services & Support	France

b) In case the use of a Subprocessor has been authorized by the Controller, the Processor shall enter into a written contract with the Subprocessor ("**Subprocessing Agreement**") and such Subprocessing Agreement shall (i) impose upon the Subprocessor the same obligations as imposed by this DPA upon the Processor, to the extent applicable to the subcontracted Services, (ii) describe the subcontracted Services, and (iii) describe the technical and organizational measures the Subprocessor has to implement pursuant to Annex 2, as applicable to the subcontracted Services. The Controller has the right to request a copy of the Subprocessing Agreement.

c) Where the Subprocessor fails to fulfil its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of the Subprocessor's obligations.

d) In case a Subprocessor is located outside the EU/EEA in a country that is not recognized as providing an adequate level of data protection, the Processor will ensure that the Controller and the Subprocessor enter into a direct data processing agreement based on EU Standard Contractual Clauses as provided by the EU Commission Implementing Decision (EU) 2021/914 of June 2021 (Module 3 - Processor to Processor).

9 Limitation on Liability

a) Each party is responsible for discharging the obligations incumbent on them in this order-processing contract and under applicable data protection law.

b) Each instance of liability that relates to this data processing agreement or that arises from an infringement of obligations under it or under applicable data protection law is subject to the liability provisions established in, or applicable to, the service contract, unless this order-processing contract provides otherwise. Where liability is subject to the liability provisions established in, or applicable to, the service contract, the liability that has arisen from this data processing agreement is to be deemed as having arisen from the corresponding service contract for the purpose of calculating maximum liability or of establishing the applicability of other liability limits.

10 Exemption from Liability

The contractor exempts the legal entity ("controller") and its executive and supervisory board members, employees, legal successors and representatives from all claims, damages, losses, costs, fines and other expenses (including, in particular, reasonable attorney fees and legal costs) arising from, or as a consequence of, a claim, demand, lawsuit, court order, or other proceedings brought by third parties (including a regulatory body) as a result of, or in connection with, an infringement by the contractor of its obligations under this data processing agreement.

11 Term and termination

The term of this DPA is identical with the term of the Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Agreement. If the contractor is active in connection with several contracts / orders this DPA ends with the end of the last contract / order by the contractor for the Controller.

12 Miscellaneous

a) The Parties are required to comply with those obligations under the GDPR and under any other applicable data protection laws that apply, as applicable, to the Controller in its role as data controller or to the Processor in its role as data processor.

b) If and to the extent necessary to comply with mandatory provisions regarding the commissioning and performance of the Parties under the laws applicable to the Parties, each Party may require any necessary changes (including amendments) to the provisions of this DPA and its annexes.

c) This DPA shall be governed by the same law as the Agreement except as otherwise stipulated by applicable data protection law. The place of jurisdiction for all disputes regarding this DPA shall be as determined by the Agreement except as otherwise stipulated by applicable data protection law.

d) In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the Parties' data protection obligations, this DPA shall prevail.

e) Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or – should this not be possible – (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this DPA contains any omission.

The parties hereto have executed this Agreement with the intent that it be effective on the date when mutually signed

unless agreed otherwise.

Controller	**Rencore (Processor)**
By: _____ (Authorized Signature)	By: _____ (Authorized Signature)
Name: _____	Name: _____
Title: _____	Title: _____
Date: _____	Date: _____

Annex 1

1 Categories of data subjects

The personal data processed concern the following categories of data subjects:

- User context
- Service context

2 Subject-matter of the processing

Rencore Governance is storing the following data:

2.1 User context

End-users of the service

- user names
- user id
- email addresses

2.2 Service context

Data that is collected from Microsoft 365 by connecting the service to the Controllers tenant

- URLs
- titles
- metadata of objects (no user context)

from collected data (e.g. Site Collections, Sites, Lists, Teams).

All collected data / logs are encrypted using built-in Azure encryption.

More details around the software architecture and process can be found at:

- https://docs.rencore.com/governance/technical-documentation/rencore-governance-architecture
  https://docs.rencore.com/governance/technical-documentation/scanning-and-throttling

In case any data should not be scanned it is possible to enable/disable specific services (e.g. Azure AD Auditing)

2.3 Nature and purpose of the processing

The aforementioned personal data is processed by Rencore Governance in the course of providing the Software-as-a-Service, as detailed in the product description for Rencore Governance, as well as for the purposes of providing support for these services, billing for these services, assessing product usage, and providing a satisfactory user experience in the form of user guides and user feedback options, with the latter processing activities being optional (please also refer to our list of Sub-processors for further information). Rencore Governance and Rencore as a company have no direct control over the user work behaviour and do not process any personal data independent of processes commenced by the Customer (e.g. using the tool, requesting support for the tool, etc.) So that Rencore can contact users based on integrated and configured violations rules, the personal data of the affected users (names and email addresses) are stored. No other processing activity takes place within Rencore Governance.

The Customer can request the deletion of data at any time (with exceptions where continued processing is necessary for the maintenance of the contract between the Customer and Rencore or for other legal reasons, e.g. billing data). The Customer can delete data within their Rencore Governance instance at any time, including in preparation for terminating the services. Workspaces are deleted 30 days after they have been set for deletion, in order to allow for recovery of accidentally deleted workspaces within those 30 days.

2.4 Categories of personal data

The personal data processed by Processor on behalf of Controller concern the following categories of personal data: https://docs.rencore.com/governance/technical-documentation/security-and-privacy/data/personally-identifiable-information

2.5 Special categories of data

n/a

Annex 2

Description of the technical and organizational measures implemented by Processor in accordance with applicable data protection law:

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement the following technical and organizational measures to ensure a level of security appropriate to the risks for the rights and freedoms of natural persons. In assessing the appropriate level of security the Controller and the Processor took account in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

1 Pseudonymization

The following measures shall be implemented to address the pseudonymization of the personal data:
In order to achieve the purposes of the commissioned data processing it is not possible to pseudonymize the personal data at this moment.

2 Encryption

The following measures shall be implemented to address the encryption of the personal data:
In Rencore Governance, all information is encrypted. Azure Storage Accounts have built-in support for encryption at rest, and in-transit. In addition to this, we add another layer of cryptographic AES 256-bit industry-standard encryption around the data before it is transmitted to the storage. All transmission from the application to the end-user are **SSL** encrypted.

Read more about in our Knowledge Base about https://docs.rencore.com/governance/technical-documentation/security-and-privacy/is-rencore-governance-secure

3 Confidentiality of the processing systems and of the services

The following measures shall be implemented to address the confidentiality of the processing systems and of the services:

Only authorized personnel have access to production systems where personal data exist or are processed.

4 Integrity of the processing systems and of the services

The following measures shall be implemented to address the integrity of the processing systems and of the services:

- Audit logs are kept for Rencore systems, including access to processing- and cloud environments.
- Only authorized personnel at Rencore can access the audit logs.

5 Availability of the processing systems and of the services

The following measures shall be implemented to address the availability of the processing systems and of the services:

- Rencore Governance performs regular backup of all configuration data.
- Rencore complies with GDPR regulations, and processes personal data accordingly.

6 Resiliency of the processing systems and of the services

The following measures shall be implemented to address the resiliency of the processing systems and of the services:

- 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 are running multiple instances to distribute and load balance the incoming requests.

7 Ability to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident

The following measures shall be implemented to address the ability to restore the availability and access to the personal data in a timely manner in the event of a physical or technical incident:

- We adhere to our Rencore Backup Policy for data backups.
- Rencore Governance has regular backups of configuration, and the infrastructure can be replicated in the same, or new regions, in case 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, we might be impacted by this during technical incidents.

8 Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures

The following measures shall be implemented to address the regularly testing, assessing and evaluating of the effectiveness of technical and organizational measures:

- Rencore has started to implement organizational policies to target a SOC2 compliance standard, which will enable us to undergo regulatory audits. A SOC2 audit mandates that we have valid security policies, risk assessments, annual reviews, external audits, and more. This is a work in progress.

9 Ensuring the Confidentiality of Processing Systems and the Contractor’s Services

The contractor adopts the following security measures to ensure the confidentiality of processing systems and the services it performs:

- All systems are configured according to security best practices.

10 Integrity of Processing Systems and the Contractor's Services

The contractor adopts the following security measures to ensure the integrity of processing systems and the services it performs:

- All systems are configured according to security best practices.

11 Availability of Processing Systems and the Contractor's Services

The contractor adopts the following security measures to ensure the availability of processing systems and the services it performs:

- All systems are configured to be available during high load.

12 Resilience of Processing Systems and the Contractor's Services

The contractor adopts the following security measures to ensure the resilience of processing systems and the services it performs:

- All systems are built cloud-native as resilient applications, and adopts security best practices.