Software-as-a-Service Agreement

This Software-as-a-Service Agreement (the "**Agreement**") is made between

[Company Name, Address]

(hereinafter "**Customer**")

and

Rencore GmbH

Bayerstrasse 71-73

80335 Munich

Germany

(hereinafter "**Rencore**")

(Customer and Rencore, hereinafter each a "**Party",** together the "**Parties**"):

WHEREAS, Rencore is a software provider providing a product ("**Rencore Governance**") that connects and integrates with Microsoft 365, Microsoft Azure and other workspace solutions operated by the Customer (together the "**Customer Services**");

WHEREAS, Customer wishes to use Rencore Governance;

WHEREAS, Rencore intends to provide Customer Rencore Governance by way of a software-as-a-service (SaaS).

Therefore the Parties agree as follows:

1 Scope of this Agreement and general provisions

1.1 Definitions

In this Agreement, the following definitions shall apply:

Term	Definition
API	Application Programming Interface: code that allows for two computer programs to communicate with one another.
Availability	Is defined in Clause 2.3.1.
BGB	is defined in Clause 1.8.
Confidential Information	is defined in Clause 11.2.2.
Contractual Arrangements	is defined in Clause 13.4.1.
Customer	is defined on the front page.
Customer's Affiliates	is defined in Clause 1.4.1.
Customer Data	is defined in Clause 4.1.1.
Customer Services	is defined on the front page.
Customer Success Manager	is defined in Clause 12.1.2.
Disclosing Party	is defined in Clause 11.2.2.
Documentation	is defined in Clause 2.4.
Downtime	is defined in Clause 2.3.4
Effective Date	is defined in Clause 1.5.2.
GDPR	is defined in Clause 11.1.1.
Party / Parties	is defined on the front page.
Receiving Party	is defined in Clause 11.2.2.
Rencore	is defined on the front page.
Rencore's Affiliates	is defined in Clause 1.9

Term	Definition
Response Time	is defined in Clause 3.3.3.
SaaS-Services	is defined in Clause 1.4.1.
Service Description	is defined in Clause 2.1.1.
Service Hours	is defined in Clause 3.2.5.
Service Order	is defined in Clause 1.5.1
Services	is defined in Clause 1.3.1.
Severity Level	is defined in Clause 3.2.7.
Support-Services	is defined in Clause 1.4.2.
Trial-Services	is defined in Clause 10.
Working Days	is defined in Clause 2.2.4.

1.2   Interpretation and Construction

The headings will not be taken into consideration for the interpretation of this Agreement. The Annexes and their Schedules form an integral part of this Agreement. References to this Agreement also include its Annexes and their Schedules as well as any later supplementary or amendment agreements. References to Annexes of this Agreement also include their Schedules.

1.3   Scope of this Agreement

1.3.1   This Agreement governs the terms and conditions for the provision of the SaaS-Services and the Support-Services as defined in Clause 1.4 (together the "**Services**") by Rencore to Customer.

1.4   Services provided by Rencore

1.4.1   As of the Effective Date and during the term of the applicable Service Order Rencore shall enable Customer and its affiliates within the meaning of Sections 15 et seq. German Stock Corporation Act ("**Customer's Affiliates**") to use Rencore Governance as further specified in the applicable Service Order on a software-as-a-service basis in accordance with Clause 2 (the "**SaaS-Services**").

1.4.2   As of the Effective Date and during the term of the applicable Service Order Rencore shall also provide Customer and Customer's Affiliates support for the SaaS-Services in accordance with Clause 3 (the "**Support-Services**").

1.5   Service Orders

1.5.1   The Services shall be provided on the basis of an order placed by Customer if and to the extent accepted by Rencore (the "**Service Order**"). This Agreement alone creates neither an obligation on the part of Customer to place Service Orders nor an obligation on the part of Rencore to provide certain Services. Rencore will be entitled and obliged to provide, and Customer will be entitled and obliged to accept and pay, Services only if and only to the extent that the Parties have agreed on the provision of specific Services under a Service Order.

1.5.2   Service Orders are considered agreed between the Parties and enter into effect when Rencore receives a purchase order from the Customer that confirms the Customer's acceptance of the agreed contractual terms, or the Customer digitally signs a quote generated by Rencore's CRM system. Service Orders are also considered agreed on the completion of the checkout process in https://my.rencore.com. The date from which the SaaS-Services will be provided ("**Effective Date**") will be stated in the quote for the Service Order, the Service Order itself or any other document regarding the start of the provision of the SaaS-Services agreed by the Parties. This form is without prejudice to any additional statutory requirements or requirements explicitly agreed by contract between the Parties for a specific Service Order to be effective, especially conditions and approval requirements.

1.5.3   Each Service Order incorporates the terms of this Agreement by way of reference.

1.5.4   This Agreement, in particular Sec. 10, also applies to the provision of Trial-Services by Rencore to Customer, taking into account the exceptions outlined in Sec. 10.

1.6   Incorporation of other provisions

1.6.1   A provision of this Agreement or of a Service Order can be validly supplemented, modified, replaced and/or deleted only if and to the extent that this is agreed between Rencore and Customer and if the clause or document to be supplemented, modified, replaced and/or deleted is either explicitly or by reference to a set of rules or to a document specifically designated.

1.6.2   Any general terms and conditions of the Parties do not apply to the provision of the Services under this Agreement. This even applies if an offer of either Party and/or a Service Order refers to such general terms and conditions and the other Party does not explicitly object to the application thereof prior to or when signing or accepting a Service Order.

1.7   Order of precedence of the various sets of rules

The following order of precedence applies between the various sets of rules applicable to a Service Order:

1.   Service Order

2.   Annexes to a Service Order (if any),

3.   Data Processing Addendum for the Agreement (**Annex 2** to this Agreement),

4.   The main body of this Agreement,

5.   Annexes to this Agreement,

6.   Schedules to an Annex of this Agreement.

Unless explicitly agreed otherwise, the set of rules with the lowest rank number shall be decisive in the event of conflicts or inconsistencies between the sets of rules in each case.

1.8   Retention of title

Any transfer of ownership to objects or rights (especially rights of use under Clause 2.5) which is owed by Rencore to Customer under a Service Order is subject to the condition precedent (Section 158 (1) German Civil Code (*Buergerliches Gesetzbuch* – "**BGB**")) of full payment of the remuneration owed with respect to the relevant Service Order.

1.9   Sub-contractors

Without prejudice to its obligations under Clause 11.1.1 and the Data Processing Addendum for the Agreement (**Annex 2**), Rencore is free to use sub-contractors to render its Services at its own discretion. That applies in particular to Rencore's affiliates within the meaning of Sections 15 et seq. German Stock Corporation Act ("**Rencore's Affiliates**").

1.10   Responsibility for affiliates

For the purpose of this Agreement and all Service Orders concluded hereunder, each Party is responsible for fault on the part of its affiliates to the same extent as for fault on its own part; Section 278 BGB applies *mutatis mutandis* to all affiliates of the Parties.

2   SaaS-Services

2.1   Provision of the SaaS-Services

2.1.1   During the term of a Service Order, Rencore will make the SaaS-Services agreed in the applicable Service Order available to Customer. The SaaS-Services will be rendered as described in the service description contained in **Annex 1** (the "**Service Description**") and in accordance with generally accepted technical and quality standards. The SaaS-Services will be governed by the statutory provisions of the law on service contracts, Sections 611 et seq. BGB, unless this Agreement or the applicable Service Order provides otherwise.

2.1.2   Rencore provides Customer and Customer's Affiliates access to the SaaS-Services to be provided over the Internet. Customer acknowledges that Rencore does not control the transfer of data over telecommunications facilities, including the Internet.

2.1.3   The SaaS-Services are a product that connects to and integrates with business apps that the Customer must purchase separately from the providers of these business apps. The SaaS-Services technically rely on these business apps to function as intended. Rencore is therefore not responsible if and to the extent a failure to perform the SaaS-Services in accordance with this Agreement is caused by non-availability or malfunctioning of the relevant business apps and/or any related services.

2.1.4   Except for the express obligations set forth in this Agreement and any Service Orders, Rencore assumes no obligations to Customer, and any statements about the SaaS-Services and their respective functionality in any communication with Customer are for information purposes only and do not constitute obligations of Rencore unless explicitly agreed otherwise. None of Rencore's obligations under this Agreement or a Service Order shall be deemed to constitute a guaranteed quality or other guarantee. Furthermore, Rencore assumes no warranty or liability that the SaaS-Services meet the expectations of Customer with regard to individual requirements and purposes of Customer unless explicitly agreed between the Parties in this Agreement or in a Service Order.

2.2   Changes to the SaaS-Services

2.2.1   Rencore may (i) make changes or updates to the SaaS-Services including enhancements or other changes (such as functionality, infrastructure, security, technical configurations, application features, etc.), and (ii) make the corresponding changes or updates to the Service Description to reflect such changes or updates to the SaaS-Services.

2.2.2   Minor feature changes and/or removals that will not result in a material reduction of functionalities or level of performance, security or availability of the originally agreed SaaS-Services may be carried out without prior communication to or approval of the Customer.

2.2.3   Rencore will provide Customer with the updated version of the Service Description in the form of release notes available within the product and under the following link: https://url.rencore.com/gov-releasenotes.

2.2.4   "**Working Days**" are all days except Saturdays, Sundays and public holidays in Bavaria, Germany.

2.2.5   The SaaS-Services depend on the free APIs provided by third-party cloud service providers (e.g. Microsoft 365 Graph) to connect the SaaS-Services to the Customer Services. If these third-party cloud service providers determine that the APIs can no longer be accessed for free, or limit the capacity of accessing the APIs for free to below the required capacity to operate the SaaS-Services, Rencore may require that the Customer bears the additional costs that are charged by the third-party cloud services provider pertaining to the use of these APIs. This will be listed as a separate item in any invoice that the Customer receives for SaaS-Services.

2.3 Availability of the SaaS-Services

2.3.1 Rencore warrants (*gewaehrleistet*) that the SaaS-Services are at least 99.5% available in each period of 90 days during the term of the applicable Service Order (the "**Availability**").

The demarcation point, at which the Availability will be measured, shall be the WAN-sided router output of the data centre in which the SaaS-Services are hosted. For this purpose, Rencore makes use of its own availability tracking tool, available under https://status.rencore.com.

2.3.2 The actual availability is calculated as follows:

$$\frac{129,600 \ minutes - \ Downtime \ in \ minutes}{129,600 \ minutes} \ \text{in percent (\%)}$$

This is subject to exceptions listed in the following clauses.

2.3.3 Availability is recorded 24 hours, 7 days per week, subject to exceptions listed in the following clauses.

2.3.4 The "**Downtime**" is the total number of minutes within 90 days during which the SaaS-Services are not accessible to Customer and/or Customer's Affiliates for use over the Internet. The Downtime does not include periods of inaccessibility of the SaaS-Services (i) that are outside of the standard worktimes of the Customer (09:00-17:00 in the time zone in which the Customer usually operates, unless communicated otherwise by the Customer) or (ii) that are due to factors beyond Rencore's control, for example due to (a) unforeseeable events, IT security incidents or outages of connected services, (b) other services agreed upon with the Customer that prevent access to the SaaS-Services, (c) service degradation of third-party cloud providers (e.g., Microsoft, Cloudflare, etc.), and their services (Azure, Microsoft 365, Azure Active Directory/Authentication, Global DNS, etc.) and/or (d) periods of unavailability due to maintenance of the SaaS-Services in accordance with Clause 2.3.5.

The Customer understands that the SaaS-Services provided are a non-essential service that must be actively used by the Customer.

2.3.5 Maintenance of the SaaS-Services shall not be deemed as Downtime if (i) Customer is notified at least 72 hours prior to the beginning of the maintenance (email being sufficient) and (ii) the maintenance conducted during the standard worktimes of the Customer (09:00-17:00 in the time zone in which the Customer usually operates, unless communicated otherwise by the Customer) does not cause an outage lasting longer than 360 minutes over the course of the respective 90 days. Maintenance of the SaaS-Services shall also not be deemed as Downtime if the maintenance is mutually agreed upon with the Customer. Maintenance of the SaaS-Services shall also not be deemed as Downtime where the reason for the work is not the failure on the part of Rencore to meet obligations regarding the provision of Cloud Services (force majeure and/or unavailability of third-party services).

2.3.6   At Customer's request, for each 90 days in which Availability is not met, Rencore shall issue a credit to Customer in the amount of 1% of the service fees owed by Customer according to the applicable Service Order for the respective 90 days for each fractional percentage point below the Availability pursuant to Clause 2.3.1, whereby the total amount of the credits per 90 days may not exceed a total of 20% of the service fees owed by Customer for the respective 90 days. The credits must be requested by Customer within 90 days following the 90-day period of time over which Availability is not met. The credits are deducted from the next invoice issued to Customer following its request.

2.3.7   Other rights of Customer in the event of a failure in meeting the Availability under applicable law remain unaffected.

2.4   Documentation for the SaaS-Services

Rencore will (at no additional charge) provide Customer access to all generally available user documentation for the SaaS-Services (the "**Documentation**"). This Documentation takes the form of an online Documentation and is available here: https://docs.rencore.com/governance/. The Documentation is sufficient to enable Customer's personnel to use and implement the SaaS-Services.

2.5   Rights of use

2.5.1   Rencore reserves all rights to the SaaS-Services, including all associated property rights. Customer shall not be granted any rights under herein.

2.5.2   Rencore hereby grants to Customer and Customer's Affiliates a non-exclusive, non-sublicensable, non-transferable, territorially not restricted right to use the SaaS-Services during the term of the applicable Service Order for their own business purposes. Own business purposes of Customer for the purposes of this Clause 2.5 are also deemed to include business purposes of Customer's Affiliates.

2.6   Suspension of access to the SaaS-Services

2.6.1   Rencore may suspend Customer and/or Customer's Affiliates access to the SaaS-Services in whole or in part, if Rencore has legitimate reason to assume that the usage of the SaaS-Services by Customer and/or Customer's Affiliates (i) is materially not in compliance with this Agreement or the applicable Service Order, or (ii) violates applicable laws, or (iii) has a negative effect on the rights or legitimate interests of Rencore, Rencore's Affiliates or third parties so that immediate action is necessary to avoid damage.

2.6.2   Rencore will limit the suspension to the extent and period of time necessary for the elimination of the reason for the suspension. Rencore will inform Customer prior to any intended suspension specifying a period for relief (email being sufficient). Such notification of Customer is not necessary if special circumstances are given which, when the interests of both Parties are weighed, justify immediate suspension. In any case, Rencore will notify Customer immediately after suspension (email being sufficient). The suspension right is in addition to, and restoration is without prejudice to, all other rights and remedies Rencore may have.

3　Support-Services

3.1　Applicable law

Support will be governed by the statutory provisions of the law on service contracts, Sections 611 et seq. BGB, unless this Agreement or the applicable Service Order provides otherwise.

3.2　1st level Support Services

3.2.1　As part of 1st level support, Rencore shall provide advice and support to Customer and Customer's Affiliates for the configuration as well as operation of the SaaS-Services. The 1st level support is also responsible for receiving all requests for support. The 1st level support consists of the following services:

- Recording and confirming a support request from Customer or Customer's Affiliates;

- Analysing the content of the support request;

- Resolving the support request, if possible with the standard application/system functionalities;

- Forwarding the support request to the 2nd level support, if applicable.

3.2.2　The 1st level support consists of staff who can speak German and/or English who are familiar with the standard functions of the SaaS-Services.

3.2.3　Customer can contact the 1st level support at any time via Rencore's designated support contact details and open a support ticket. The support request will be processed within the Service Hours.

3.2.4　During the Service Hours, Customer can also contact 1st level support by a chat system within the application. Rencore shall provide Customer with the relevant contact details and relevant information about their subscription, in accordance with Clause 3.3.1.

3.2.5　Rencore's "**Service Hours**" are on Working Days, 9:00 to 17:00 CET.

3.2.6　Subject to Clause 3.3.1, all requests for support are classified by Rencore according to the Severity Levels defined in Clause 3.2.7.

3.2.7　Four "**Severity Levels"** are distinguished:

- Severity Level 1 – "Critical"

- Severity Level 2 – "Major"

- Severity Level 3 – "Minor"

- Severity Level 4 – "Low"

The requests for support are assigned to these four Severity Level categories on the basis of the following criteria:

- Severity Level 1: The request for support is so important that without its immediate resolution, (i) the continued operation of Customer's business is at risk in whole or in part, or (ii) the appropriate use of the SaaS-Services, or a substantial part of them, is not possible.

- Severity Level 2: The request for support is very important for Customer's business operations, so that without its timely resolution (i) Customer's business operations are significantly disrupted or (ii) the appropriate use of the SaaS-Services, or a substantial part of them, is only possible with significant restrictions.

- Severity Level 3: The reason for the support request (i) influences the operations of Customer's business, but allows for proper operations with slight limitations, or (ii) the appropriate use of the SaaS-Services, or some of them, is slightly restricted.

- Severity Level 4: All support requests that do not fall under Severity Levels 1 to 3.

3.3 Transmission of support requests

3.3.1 To report a security incident the Customer shall describe it in text form to security@rencore.com; to report an issue with the SaaS-Services, the Customer shall describe it in text form to support@rencore.com . The Customer shall explain how and when the incident occurred, which measures have been tried already to resolve it, instructions and if possible screenshots on how to reproduce it, and information as to whether only specific or all users are affected. When reporting an incident, the Customer shall identify the individuals affiliated with the Customer whom Rencore may contact regarding the incident in question and indicate how these individuals can be reached by phone or email. The Customer shall name contact persons who are available for Rencore to contact throughout the duration of the incident and at least during the Customer business hours.

3.3.2 Rencore shall start processing the support request within the Response Times referred to in Clause 3.3.3 and provide the Customer with an initial proposal for resolution or for the further processing of the support request.

3.3.3 The allocated "**Response Time**" is to the end of the next business day if troubleshooting attempts commence during the course of a business day; if the request for support is made outside of support hours, the allocated "**Response Time**" is two business days.

3.4 2nd level support

3.4.1 Rencore shall provide Customer with 2nd and 3rd level support to provide advice and assistance on the configuration and operation of the SaaS-Services.

3.4.2 Customer cannot directly contact the 2nd or 3rd level support. In the 2nd and 3rd level support, specialists, in particular Rencore's developers and engineers, handle and resolve Customer's support requests that were not resolved by the 1st level support.

3.5 Services not included

3.5.1 The following services are not included in the Support Services specified in this Clause 3:

- Training;

- Remedying of errors/malfunctions of the SaaS-Service caused by Customer as a result of improper acts or omissions;

- Development services;

- Setup/implementation of the SaaS-Services;

- Connecting third-party services to Rencore Governance.

4 Data of Customer and Customer's Feedback

4.1.1 All data transmitted to the SaaS-Services by Customer and Customer's Affiliates ("**Customer Data**") may be used by Rencore to provide the SaaS-Services and to prevent or address security, support or technical issues only.

4.1.2 Without prejudice to Rencore's obligations under Clause 11.1.1 and the Data Processing Addendum for the Agreement (**Annex 2**), Rencore and its sub-contractors may collect anonymised data on the use of the SaaS-Service by Customer and Customer's Affiliates to compile statistical and performance information related to the provision and operation of the SaaS-Services and may use such information at their own discretion, particularly for the development of the SaaS-Services and to prevent or address security, support or technical issues.

4.1.3 Customer grants Rencore and Rencore's Affiliates a non-exclusive, sublicensable, transferable, timely unlimited, irrevocable, territorially not restricted, royalty free right to use or incorporate into the SaaS-Services any suggestions, enhancement requests, recommendations or other feedback provided by the Customer relating to the operation of the SaaS-Services.

5 Third party rights

5.1.1 In providing the Services, Rencore is obliged to respect third party rights (for example copyrights and other IP rights). In particular, the exercise of the rights of use granted by Rencore hereunder may not be impaired by any third-party rights.

5.1.2 If a third party asserts claims against Customer or Customer's Affiliates alleging that the use of a Service infringes any rights to which such third party is entitled (for example, infringement of IP rights), Rencore shall indemnify and hold Customer and/or Customer's Affiliates harmless from such claims and take on the responsibility and control of all actions required to defend such claims at the expense of Rencore. If

Rencore does not defend such claims, or does not defend such claims in a proper manner or to the extent required, Customer and Customer's Affiliates may take any action required for the defence itself. Customer and Customer's Affiliates shall not acknowledge any claims asserted by third parties, or enter into any settlement agreement in respect thereof, without the prior written consent (*Schriftform*) of Rencore. In turn, Rencore shall not enter into any settlement agreements providing for any duties on the part of Customer or Customer's Affiliates relating to conduct or performance without the prior written consent (*Schriftform*) of Customer. Consents shall not be unreasonably withheld or delayed.

5.1.3   Customer shall inform Rencore without undue delay if Customer or a Customer's Affiliate is held liable on account of an infringement of third-party rights by using a Service. The Parties shall provide each other with the information required for defending such claims.

5.1.4   Rencore shall reimburse Customer and Customer's Affiliates for any expenses incurred by them in connection with the defence of the claims as described in Clause 5.1.2 sentence 1 to the extent that accruing such expenses was reasonable. Rencore is not required to reimburse expenses where Customer or the relevant Customer's Affiliate is reimbursed for such expenses by the third party.

5.1.5   In the event of an IP infringement, Rencore may in its reasonable discretion either (i) alter the relevant Service or the relevant part thereof affected by the IP infringement or replace it by another equivalent Service or the relevant part thereof so that third party rights are no longer infringed, or (ii) procure from the third party the rights required to deliver the Service or the relevant part thereof in conformity with the applicable Service Order. Rencore is not entitled to alter the relevant Service or the relevant part thereof pursuant to this Clause 5.1.5 (i), if such alteration is unreasonable (*unzumutbar*) for Customer.

5.1.6   When using the SaaS-Services Customer is obliged to respect all third-party rights (for example copyrights and other IP rights) and applicable laws. Clauses 5.1.2 to 5.1.5 apply *mutatis mutandis* for the benefit of Rencore.

6   Remuneration

6.1   Service Fees

6.1.1   The service fees to which Rencore is entitled for the provision of the SaaS-Services are specified in the applicable Service Order.

6.1.2   Unless otherwise expressly provided for in the applicable Service Order, the service fees are payable in advance for the agreed service period. Price adjustments may be made mid-service period where additional licence bundles are purchased and/or in the event of overusage of licences for a period of more than 30 days.

6.1.3   Rencore may increase the service fees referred to in Clause 6.1.1 by means of a text statement to Customer with effect from the end of the currently purchased service period.

6.1.4   Unless otherwise expressly provided for in the applicable Service Order, the remuneration for the Support-Services is included in the service fees.

6.1.5   Any and all service fees payable under this Agreement or a Service Order are exclusive of any and all taxes, levies or duties of any nature, including, but not limited to, value-added, sales, use, or withholding taxes, assessable by any local, state, federal, or foreign jurisdiction.

6.1.6   As referenced in Clause 2.2.5, any additional costs as a result of APIs that connect the SaaS-Services to Customer Services no longer being free may be borne by the Customer, and will be listed separately in the relevant invoice.

6.2   Invoices, discount and interest

6.2.1   Unless otherwise expressly provided for in the applicable Service Order, all payments are to be made in EUR or USD (as selected by the Customer) and are payable upon commencement of Services by credit card, a wire transfer or an alternative payment system as prescribed by the Customer.

6.2.2   For late interest and default, the statutory provisions apply.

6.3   Right of retention

Customer can exercise a right of retention, a right to refuse performance or a right of setoff only to the extent that the counterclaim has been established by final judgement or is not disputed by Rencore.

7   Customer's Cooperation

7.1   General cooperation duties

Customer shall render to Rencore any cooperation that is reasonable (*zumutbar*) to Customer for the proper performance of the Services. The Customer acknowledges that the provision of the Services may depend on Customer's timely and proper performance of its cooperation obligations. Customer shall (i) in particular carry out the acts of cooperation agreed in a Service Order, (ii) make available to Rencore the data and information that is necessary for rendering the agreed Services, particularly the Support-Services, and (iii) if Customer claims a defect of the SaaS-Services, provide Rencore with all information available to Customer regarding the claimed defect.

7.2   Access to Customer Services

Customer acknowledges that it is a prerequisite for the proper performance of the SaaS-Services that Customer provides the SaaS-Service with access via an API to the relevant structures, inventories and metadata in the Customer Services, so that the SaaS-Service can conduct the relevant scans and exercise the relevant workflows. Such access is necessary and proportionate for the basic functions of the SaaS-Service. The details of this access are provided both in the SaaS-Service's Documentation and in the Data Processing Addendum for the SaaS Agreement.

8   Liability

8.1   Liability on the merits

Rencore will be fully liable for damages and futile expenses only to the extent such damages or expenses are due to any intentional (*Vorsatz*) or grossly negligent (*grobe Fahrlaessigkeit)* conduct of Rencore, its legal representatives or vicarious agents.

8.2   Liability in terms of amount

8.2.1   In the event of a slightly negligent (*leichte Fahrlaessigkeit*) breach of a material contractual duty (*wesentliche Vertragspflicht*) by Rencore, its legal representatives or vicarious agents, liability of Rencore is limited to (i) in each event of damage an amount corresponding to 30% of the total remuneration owed by Customer pursuant to the relevant Service Order in the contractual period (as defined in the Service Order) in which the relevant event of damage occurs, and (ii) for all events of damage caused within the scope of a Service Order falling in the same contractual period, a total amount corresponding to 100% of the remuneration owed by Customer for the Services under the relevant Service Order in the year in which the relevant events of damage occurs.

8.2.2   Material contractual duties for the purposes of this Clause are all duties the fulfilment of which enable the proper performance of a Service Order in the first place and on the compliance with which the Customer usually relies and may rely, and the breach of which jeopardizes the achievement of the Service Order's purpose.

8.2.3   The availability of critical APIs provided by third-party cloud service providers is not to be considered a material contractual duty of Rencore, as this is outside of the sphere of influence of Rencore; however, clause 12.3.2 provides alternative remedy for the event of the unavailability of critical APIs in the form of a special termination right.

8.3   Liability for pre-existing defaults

Any no-fault liability (*verschuldensunabhaengige Garantiehaftung*) of Rencore as provided in Section 536a (1) Alt. 1 BGB for pre-existing defects is excluded. However, the foregoing is without prejudice to Rencore's liability for pre-existing defects in case of a culpable breach of duty (*schuldhafte Pflichtverletzung*) of Rencore in accordance with Clauses 8.1 and 8.2.

8.4   Mandatory liability

The foregoing shall not affect liability for damages resulting from an injury to life, body or health. The same applies to claims resulting from warranty breaches (*Verletzung von Garantien*), and claims under the German Product Liability Act (*Produkthaftungsgesetz*).

9   Limitation

9.1.1   Except for claims for damages for which Rencore is liable according to Clauses 8.1 sentence 1 and 8.4, the limitation period for any claims which Customer may have against Rencore under or in connection with claims arising from any legal relationship between the Parties governed by this Agreement is two (2) years from the end of the calendar year during which such claim arose and Customer became aware of the circumstances giving rise to the claim and the identity of the debtor or should have become aware thereof without gross negligence. Sentence 1 shall also apply to claims due to non-performance or insufficient performance of a claim for cure of Customer.

9.1.2   If and to the extent that statutory provisions provide for a limitation period for the benefit of Rencore which is shorter than the limitation period provided for in Clause 9.1.1, such shorter limitation period shall apply.

10   Specific provisions for Trial-Services

         If and to the extent that the SaaS-Services or parts thereof (e.g. new features) are provided to Customer for trial purposes at no (additional) charge (the "**Trial-Services**"), the statutory provisions of the law on gratuitous loans, Sections 598 et seq. BGB apply, unless this Agreement or the applicable Service Order provides otherwise. Rencore's liability is limited to intent and gross negligence in accordance with Section 599 BGB. If Rencore fraudulently conceals a legal defect or a defect of the Trial Services, then Rencore is liable to compensate Customer for any damage arising from this in accordance with Section 600 BGB. Clauses 2.3 and 8 do not apply to these Trial-Services and Rencore is not obliged to provide Support-Services for the duration of the Trial-Services.

11   Data protection, information security and confidentiality

11.1   Data protection

11.1.1   Any personal data which Rencore obtains or becomes aware of will be processed by Rencore within the limits of the applicable data protection laws. Rencore is in particular obliged to observe and comply with the provisions of the General Data Protection Regulation ("**GDPR**").

11.1.2   When entering into this Agreement, the Parties also conclude the Data Processing Addendum for the Agreement as per **Annex 2**. At Customer's request, Rencore will enter into a comparable data processing agreement with Customer's Affiliates using the SaaS-Services.

11.2   Confidentiality

11.2.1   Subject to the exceptions specified in Clause 11.2.6, each Party shall keep strictly confidential all Confidential Information which is made available to it by or at the instigation of the other Party in connection with the business relationship between the Parties governed by this Agreement. Furthermore, each Party shall treat said Confidential Information with the same level of care as that taken with its own Confidential Information.

11.2.2 "**Confidential Information**" is, subject to Clause 11.2.3, all information about or belonging to one Party or its affiliates, disclosed by one Party or its affiliates (the "**Disclosing Party**") to the other Party or its affiliates (the "**Receiving Party**") and which falls under one or more of the following categories:

- All data, information and work documents pertaining to the business operations, e.g. its commercial relationships, business strategies, personnel matters and/or financial affairs, of the Disclosing Party.

- All data, information and work documents pertaining to products, know-how and inventions of the Disclosing Party.

- All data, information and work documents pertaining to the IT systems used by the Disclosing Party, including but not limited to information relating to the software, hardware, and software/hardware configurations used by the Disclosing Party in the course of its business operations.

- All information which is marked or labelled with the words "confidential" or "secret" or with other words which clearly indicate that the information is confidential.

- All information which an objective recipient, exercising the care and diligence of a prudent person of business and taking into account the nature of the information and the specific circumstances and manner of its disclosure, would regard as being confidential.

- The existence and content of the Agreement and the Service Orders concluded hereunder is also classified as Confidential Information.

11.2.3 Information is not / is no longer Confidential Information insofar as

- at the time of disclosure it is, or thereafter becomes, generally available to and known by the public without an infringement of this Clause 11.2 by the Receiving Party;

- it was already known to the Receiving Party before being disclosed to the Receiving Party;

- at the time of disclosure or thereafter it is independently developed by the Receiving Party without infringing this Clause 11.2;

- the Disclosing Party has released the Receiving Party in text form from the duty of non-disclosure in a specific instance.

11.2.4 Each Receiving Party shall take all necessary steps to prevent knowledge of, access to, use and exploitation of Confidential Information by third parties. In particular, each Receiving Party shall take confidentiality and secrecy precautions that are appropriate to the circumstances and shall make the Confidential Information available to its affiliates, vicarious agents (*Erfuellungsgehilfen*) and advisors only insofar as is necessary for enabling them to perform their respective tasks (need-to-know basis). The respective Receiving Party shall bind said vicarious agents (*Erfuellungsgehilfen*) and advisors to duties of confidentiality and non-disclosure by means of a contract which are essentially comparable to the provisions contained in this Clause 11.2, if

they are not under an appropriate statutory obligation of confidentiality. Each Party shall bind its affiliates to duties of confidentiality and non-disclosure by means of a contract which are essentially comparable to the provisions contained in this Clause 11.2.

11.2.5 Subject to the exceptions defined in Clause 11.2.6 below, the Receiving Party shall not, without the prior consent of the Disclosing Party in text form,

- disclose Confidential Information to third parties other than its affiliates, vicarious agents (*Erfuellungsgehilfen*) and advisors;

- copy or reproduce Confidential Information except where necessary for the performance of this Agreement or Service Orders concluded hereunder.

11.2.6 Obtaining, use or disclosure of Confidential Information does not constitute a breach of this Clause 11.2, insofar as it is permitted or prescribed by statutory law, such as the German Business Secrets Protection Act (*Geschaeftsgeheimnisgesetz* – "**Gesch-GehG**"), or as it is necessary for the establishment, exercise or defence of legal claims.

11.2.7 The Confidential Information, including the relevant information carrier, remains the property of the Disclosing Party.

11.2.8 Confidential Information shall be deleted or returned to the Disclosing Party by the Receiving Party without undue delay if its storage is no longer necessary for the performance of this Agreement or the Service Orders concluded hereunder unless legitimate interests of the Receiving Party in further storage exist.

11.2.9 Subject to the exceptions set out in this Clause 11.2, the duty of non-disclosure of Confidential Information is unlimited as to time; that is, it will continue to apply after this Agreement is at an end.

11.3 Information security

Without prejudice to its obligations under Clause 11.1.1 and the Data Processing Addendum for the Agreement (**Annex 2**), Rencore shall take appropriate organizational and technical measures in line with the generally accepted rules of technology in order to avoid disruptions of the availability, integrity, authenticity and confidentiality of the SaaS-Services, particularly to secure Customer Data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access. An overview of the technical and organisational measures undertaken by Rencore is available as a Schedule to the Data Protection Addendum and can also be provided in addition to the Customer on request.

12 Term, termination and cancellation rights

12.1 Term and termination of a Service Order

12.1.1 The term and termination of a Service Order are primarily governed by the explicit agreements between the Parties in the applicable Service Order.

12.1.2   If there is no explicit contractual arrangement on the term of a Service Order, the relevant Service Order is deemed to have been concluded for an indefinite period of time and can be terminated by the Customer or with assistance from Customer's account manager (as assigned during the onboarding process) (**"Customer Success Manager"**) at any time prior to the end of the subscription period in their my.rencore.com customer account, effective as of the end of the current subscription period.

12.1.3   If a Service Order has been concluded for a fixed term, neither Customer nor Rencore is entitled to terminate such Service Order within that minimum term. A Service Order which has been concluded for a fixed term is extended by contractual extension periods of 12 months each time unless terminated by or on behalf of the Customer before the renewal date. Rencore reserves the right not to extend a Service Order beyond the end of a renewal date.

12.2   Term and termination of this Agreement

12.2.1   This Agreement is deemed to have been concluded for an indefinite period of time and can be terminated in writing by the Customer or with assistance from the Customer Success Manager at any time prior to the end of the subscription period of any active Service Orders, effective as of the end of the current subscription period for the last remaining Service Order.

12.2.2   The termination of a Service Order is not deemed to constitute a simultaneous termination of this Agreement, unless (i) the Party giving notice explicitly states the intention to terminate both the respective Service Order and this Agreement in the notice of termination or (ii) the Service Order terminated by the Party giving notice had been the last remaining Service Order agreed between the Parties and no other Service Orders are in effect.

12.2.3   The termination of this Agreement is deemed to constitute a simultaneous termination of all Service Orders existing between the Parties on the basis of this Agreement. The termination of such Service Orders will be effective in each case from the point in time when a separate termination of the relevant Service Order would be effective pursuant to Clause 12.1. Until such time, this Agreement shall be deemed to remain in force with respect to the relevant Service Order.

12.3   Joint provisions for the termination of a Service Order and this Agreement

12.3.1   Either Party's right to terminate a Service Order and/or this Agreement for good cause without a notice period shall remain unaffected. Good cause for the purposes of this Clause in particular (without limitation) exists if, taking into account the circumstances of the individual case and considering the interests of both Parties, the Party giving notice cannot reasonably be expected to continue a Service Order and/or this Agreement until the agreed termination date or until expiry of any regular notice period. If such good cause consists in the breach of any duty under a Service Order and/or this Agreement, notice of termination may be given only after a period fixed for remedy has expired without success or after an unsuccessful written warning. The fixing of a period may be dispensed with only for the reasons stated in sections 323 (2) BGB. The Party entitled to terminate can give notice of termination only within a

reasonable period of time from the point in time when that Party becomes aware of the cause for termination.

12.3.2   Good cause for the purposes of Clause 12.3.1 is, in particular, deemed to exist if

- proceedings are or were being conducted by the terminating Party against the other Party for the provision of information on that Party's financial situation and the assets owned by it in accordance with Sections 802c et seq. German Civil Code or similar proceedings under foreign law,

- the financial situation of either Party deteriorates significantly, or if such significant deterioration is likely to occur, and the performance owed by that Party under a Service Order is seriously jeopardised as a result thereof in a manner that can be objectively proven, or

- the SaaS-Service Availability, as defined in Clause 2.3, decreases to lower than 95% during the respective 90-day period.

- an API or multiple APIs which are required for SaaS-Services to communicate with Customer Services are no longer available, with this unavailability resulting in material disruptions to the provision of SaaS-Services.

12.3.3   Any notice of termination must be given to the other Party in text.

12.3.4   Partial terminations of only parts of this Agreement and/or parts of a Service Order are not possible.

13   Final provisions

13.1   Applicable law

This Agreement and all Service Orders concluded hereunder shall be governed by the laws of the Federal Republic of Germany to the exclusion of the United Nations Convention on Contracts for the International Sale of Goods (CISG) and the conflict of laws principles.

13.2   Jurisdiction

The courts in Munich, Germany, shall have exclusive jurisdiction over any and all disputes arising from or in connection with legal relationships governed by this Agreement, unless a provision of law mandatorily prescribes a different place of jurisdiction.

13.3   Communication details of Customer

Rencore is required to send all notifications in relation to this Agreement and/or a Service Order to the contact details of Customer specified in the applicable Service Order. Customer shall inform Rencore of any changes to its contact details.

13.4 Text form

13.4.1 Unless explicitly agreed otherwise, amendments or supplements to this Agreement, a Service Order or other arrangements which form part of the contractual relationship between the Parties in accordance with this Agreement or a Service Order (the "**Contractual Arrangements**") must be in text form, taken to mean any form in text (i.e. excluding oral communication of changes) and including electronic prompts and checkboxes, or the electronic form (elektronische Form) in accordance with section 126a BGB. The requirement of text form also applies to an agreement amending, supplementing or cancelling this Clause requiring text form; any agreement to the contrary is void.

13.5 Assignment

Subject to Section 354a, para 1 of the German Commercial Code, Customer may not assign this Agreement or any of its rights or obligations out of or in connection with this Agreement or a Service Order to a third party. The Customer's Affiliates, as defined in Clause 1.4.1, are not considered third parties.

14 Severability

14.1.1 If individual provisions in the Contractual Arrangements are invalid, the validity of the remaining Contractual Arrangements shall not be affected thereby.

14.1.2 If, applying the Contractual Arrangements in practice, gaps become apparent which the Parties did not foresee, or if any of the Contractual Arrangements is held to be invalid by final judgment or by mutual agreement of the Parties, the Parties agree to fill such gap or to replace such invalid arrangement with retrospective effect in an objective and appropriate manner and with a view to the commercial purpose of the contract and to document such agreement in text form.

--- signature page to follow ---

Annexes

Annex no.	Content
1	Service Description
2	Data Processing Addendum for the Agreement

[Place, date]   Munich, [date]

Customer   **Rencore**

[Signature]   [Signature]

_____   _____

[Name, title]   [Name, title]

_____   _____

Annex 1   Service Description

The software provided by Rencore as Software-as-a-Service is a cloud collaboration governance solution, helping Customer to stay in control of various cloud collaboration tools, such as Microsoft 365, Teams, or SharePoint through several components, such as a cloud service inventory, reporting and service management capabilities, policies and automations to help address common governance use cases.

These common governance use-cases are, among others: cloud service decluttering, cost optimisation, access review and management, user off-boarding and resource provisioning.

The supported cloud collaboration tools and the available components and governance use cases for Customer depend on the individual agreed licensing tier and the selected add-on features based on the tier and add-on definition at the time of the order. Information on the tier and add-on features that apply to your Agreement will be provided separately from the Agreement, i.e. in the Service Order.

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.

Schedules:

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)

		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 |