Data Processing Agreement

As an annex to the Agreement on SRM SW On Demand
(in the following referred to as „Service Agreement“)

between

– in the following referred to as the Customer –

Company	Onventis GmbH
Street / House number	Gropiusplatz 10
Postcode/ Place	70563 Stuttgart

– in the following referred to as the Contractor –

Company	
Street / House number	
Postcode/ Place	

Contract No.	Your contact person
Version	Contract Date

Preamble

In concluding the Service Agreement, the Parties to this Agreement enter into an agreement corresponding the requirements of the General Data Protection Regulation (EU Regulation 2016/679, hereinaft er: „GDPR“) in accordance with the Art. 28 of the GDPR. To specify the rights and obligations under the agreement for data processing in accordance with the legal obligation, the Parties hereby conclude the following agreement.

1. Scope of the Agreement

1.1. The Agreement shall apply to all activities covered by the Service Agreement and in the performance of which the Contractor's employees, or third parties acting as the Contractor's agents in accordance with this Agreement, have access to personal data for which the Customer is responsible within the meaning of Article 4 (7) of the GDPR.

1.2. In the case of regulatory conflicts between the Service Agreement and this Data Processing Agreement, the provisions of this Data Processing Agreement shall prevail.

2. Conceptual Definition

This Agreement relates only to the execution of processing of personal data (hereinafter called "data") according to Article 4(1) (definition “personal data”) and 4(2) (definition “processing”) of the GDPR by the Contractor on behalf of the Customer in the context of the fulfilment of the performance agreement (order processing). This document does constitute the assignment of additional responsibilities.

3. Type, Scope and Purpose of Data Processing

3.1. The subject and the duration of the order data processing, and the scope, nature and purpose of the proposed acquisition, processing or use of data are set out in the Service Agreement.

3.2. The following data types or categories are the object of acquisition, processing and/or use by the Contractor:

- Core personal data, for example name, address, login data, role
- Communication Data, for example telephone, e-mail
- Core corporate and product data, for example employees, addresses, bank account information, fiscal data, (for freelancers only) expertise, performance appraisal, remuneration, availability
- Core Customer data, for example, addresses, contact persons
- Log data, for example, change history, login history
- Communication data for example chats, notes, technical settings and configurations

3.3. The data subjects concerned consist of the Customer’s information about

- employees and freelancers
- suppliers
- clients
- offering or requesting companies

4. Customer's Responsibility and Authority to Issue Instructions

4.1. The Customer alone is responsible for compliance with the legal provisions of data protection laws, in particular for the legality of the transfer of data to the Contractor, and the legality of the data processing. The Customer may at any time request the release, correction, deletion and blocking of data. Should an affected person apply directly to the Contractor for the purpose of deletion or correction of his or her data; the Contractor will forward this request to the Customer as soon as possible.

4.2. The Contractor shall acquire, process, or use the data only in accordance with the instructions of the Customer. Instruction means a written notice issued by the Customer to the Contractor specifying the handling of personal data. The Service Agreement initially defines these instructions. The Customer can change, supplement or replace individual instructions by issuing additional written instructions

4.3. The Contractor shall immediately inform the Customer if the Contractor believes that a specific instruction violates any data protection provisions. The Contractor shall be entitled to suspend the implementation of the respective instruction until a person, authorized to do so on the Customer's behalf, confirms, or changes the respective instruction.

4.4. Changes to the object of processing and of procedures shall be jointly agreed and documented. The Contractor shall only provide information to third parties or the affected parties after receiving prior written agreement from the Customer. The Contractor shall not use the data for any other purposes and shall in particular not be entitled to pass the data on to third parties. The Contractor shall make no copies of personal data without the knowledge of the Customer

4.5. The Customer shall maintain a record of processing activities under its responsibility according to Art. 30 of the GDPR. The Contractor shall maintain a record of all categories of processing activities carried out on behalf of the Customer and provide this information to the Customer upon request.

4.6. Customer contact persons authorized to issue instructions pursuant to this regulation, are maintained in Annex 1: "List of Customer Contacts for Data Processing". If one of these persons, is unavailable for a prolonged period, leaves the company or for some other reason is no longer available, the Customer is obliged to appoint a replacement person and notify the other the contractor of this immediately and in writing.

4.7. The notification of directives pursuant to this regulation are to be directed to privacy@onventis.de.

5. Contractor's Obligations

5.1. In addition to the contractual provisions of this Agreement and the Service Agreement, The Contractor shall comply with all relevant legal obligations in connection with order processing.

5.2. The Contractor is obliged to maintain data secrecy. It shall be ensured that any employees involved in the processing of the data of the Customer shall be obliged to maintain confidentiality. Specifically the employees shall be obliged to maintain confidentiality of data and observe all rights and obligations of this DP Agreement, appropriate statutory confidentiality regulations as well as the provisions of the GDPR and of the German Federal Protection Act (BDSG).

This also includes the instruction on the assignment and purpose limitation existing in this order processing relationship. Upon Customer request, the Contractor will provide statements of compliance to GDPR Art. 28 (3) (b).

5.3. The Contractor shall appoint a Data Protection Officer in accordance with Section 38 of the German Data Protection Act (BDSG) and Article 37 of the General Data Protection Regulation (GDPR), who shall perform his duties in accordance with Article 39 of the DSGVO, provided that there is a legal obligation to do so. If the Contractor is not required by law to appoint a Data Protection Officer, the Contactor shall designate a member of staff responsible for data protection. The contact details of the appointed Data Protection Officer or the member of staff responsible for data protection shall be communicated to the Customer for establishing direct contact.

5.4. The Contractor shall inform the Customer immediately of any audits, investigations and measures by the regulatory authorities. The Contractor is obliged to forward requests of the data protection regulatory authorities immediately to the Customer's Data Protection Officer of the Customer or to the Customer. The Contractor will assist the Customer in the preparation of the necessary data protection documentation as well as in the response to inquiries from the data protection supervisory authorities according to the best of his abilities and for remuneration in agreement with the Customer.

5.5. Subject to a legal or official obligation of the Contractor, without corresponding instructions from the Customer, in accordance with the law of the European Union or the Member States, shall not be entitled to provide third parties or the data subject with the processed data. The Contractor is also not authorised to answer other requests from data subjects regarding the exercise of their rights under Chapter III of the GDPR without corresponding instructions from the Customer. The Contractor shall forward any such enquiries to the Customer immediately. However, in a view of the nature of the to respond to requests for the exercise of the rights concerned in processing, the Contractor shall, as far as possible, support technical and organisational measures to fulfil his obligation Chapter III of the GDPR.

5.6. The Contractor shall support the Customer in the preparation of the documentation required for this within the scope of its possibilities, insofar as the Customer cannot provide these services itself.

5.7. Taking into account the nature of the processing and the information available to him, the contractor shall assist the Customer in complying with the obligations referred to in Art. 35, 36 of the GDPR.

6. Technical and Organisational Measures and their Control

6.1. The Parties agree upon the technical and organisational security measures as laid down in the Annex 2 "Technical and Organisational Measures" to this Agreement. Annex 2 is a part of this Agreement.

6.2. Technical and organisational measures are subject to technical advances. The Contractor may thus implement adequate alternative measures. In doing so, the Contractor must achieve the level of security specified in the Annex 2 "Technical and Organisational Measures" or higher. All substantial changes shall be documented.

6.3. Upon request, the Contractor shall provide the Customer with the information required to comply with its obligation to monitor the contract and shall make the relevant evidence available. Due to the control obligation of the Customer pursuant to Art. 28 and 29 of the GDPR prior to the start of data processing and during the term of the DP Agreement, the Contractor shall ensure that the Customer can verify compliance with the technical and organisational measures taken. To this end, the Contractor shall provide the Customer with evidence of the implementation of the technical and organisational measures pursuant to Art. 32 of the GDPR upon request. Proof of the implementation of such measures can also be provided by submitting a current audit certificate, reports from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors) or a suitable certification by IT security or data protection audit (e.g. in accordance with IT baseline protection).

6.4. For inspection purposes, the Customer may inspect the Contractor's premises during normal business hours without disrupting operations to ensure compliance with this Agreement of the adequacy of the measures for compliance with the technical and organisational requirements of the data protection laws relevant to the data processing. The inspections shall be announced to the Contractor with a lead time of not less than 10 working days (Mon - Fri – excluding 24th and 31st December), in the event of a data security incident of not less than 5 working days. In doing so, the Customer must show reasonable consideration for the business processes and maintain confidentiality about the Contractor's business and trade secrets. The Contractor shall support the Customer appropriately in the monitoring of the order and provide the necessary information on request. An inspection by third parties for the Customer shall require the Contractor's prior written consent. If the Customer commissions a third party to carry out the inspection with the consent of the Contractor, the Customer shall oblige the third party in writing to maintain confidentiality, unless the third party is subject to a professional confidentiality obligation. At the request of the Contractor, the Customer shall submit the obligation agreements with the third party to the Contractor immediately. The Customer may not commission a competitor of the Contractor with the inspection.

7. Notification in Case of Offenses by the Contractor

7.1. In the event of data protection-relevant disruptions or suspected data protection violations in the processing of personal data, the Contractor shall be obliged to inform the Customer or the Customer's Data Protection Officer without delay. The Customer shall issue the necessary instructions in writing upon corresponding notification by the Contractor.

7.2. In consultation with the Customer, the Contractor shall take appropriate measures to secure the data and to mitigate possible adverse consequences for data subjects. The Contractor shall support the Customer in the fulfilment of the obligations pursuant to Articles 33, 34 of the GDPR, in particular in the preparation of the documentation required for this within the

scope of its possibilities, insofar as the Customer cannot provide these services itself.

7.3. The persons of the Customer who are to be informed in the event of such a breach are specified in Annex 1: "List of Customer Contacts for Data Processing". If one of the persons named therein is prevented from working for a longer period of time, leaves the company or is no longer available for other reasons, a replacement person must be appointed in good time and the Contractor must be informed immediately via an E-mail to privacy@onventis.de.

8. Deletion and Return of Data

8.1. Data media and data records handed over in the scope of the Agreement shall remain the Customer's property.

8.2. Upon completion of the contractually agreed services, or upon earlier request by the Customer – but at the latest on termination of the Service Agreement – the Contractor shall return any documents received, any prepared processing and use results, and any data inventories (along with any copies or replicas made thereof) related to the contractual relationship to the Customer, or destroy the same in accordance with data protection provisions and following the Customer's prior approval. The same shall apply for test and rejected materials. Upon the Customer's request, the Contractor shall provide a deletion protocol.

8.3. The Contractor must retain documentation serving as evidence of orderly and proper processing as per the respective retention periods and as required beyond the end of the contract. Alternately, the Contractor may hand said documentation over to the Customer on termination of the Agreement in order to discharge itself of this burden.

8.4. The Contractor shall remain liable for the contractual personal data after termination of this Agreement until the complete returning and/or deletion of contractual personal data according to the provisions of this agreement.

9. Subcontractor

9.1. The contractually agreed services shall be performed with the involvement of the subcontractors named in Annex 3. Furthermore, the Contractor shall only be entitled to engage further subcontractors for the (complete or partial) performance of the services owed by it (subcontracting relationships) with the prior consent of the Customer in text form. The Customer shall not refuse consent for unreasonable reasons. Consent shall be deemed to have been granted unless the Customer declares its reasoned refusal of consent in text form within a period of 5 working days from the Contractor's notification of the intended commissioning of a subcontractor. The Contractor is obliged to carefully select subcontractors according to their suitability and reliability. When engaging subcontractors, the Contractor shall commit them in accordance with the provisions of this Agreement and in doing so ensure that the Customer can also exercise its rights under this Agreement (in particular its audit and inspection rights) directly against the subcontractors.

9.2. The Customer grants the consent for the subcontractors listed in Annex 3 to this Agreement. The persons of the Customer that are to be informed in case of such an assignment of subcontractors for the consent to be given are defined in Annex 1: List of Customer Contacts for Data Processing. In the case of one of the persons named is unavailable for an extended period (e.g. has left the company, is on extended leave or for some other reason is unavailable) the Customer is obliged to appoint a replacement person and notify the Contractor via an E-mail to privacy@onventis.de.

9.3. If the subcontractor fails to comply with its data protection obligations, the Contractor shall be liable to the Customer for compliance with the obligations of that subcontractor as for its own actions.

9.4. Subcontracting relationships within the meaning of this provision do not include services which the Contractor uses from third parties as an ancillary service to support the execution of the order. These include, for example, telecommunication services, leasing of transmission paths from telecommunication providers (carriers), leasing of collocation space, maintenance and user service in the data centre, access to project management software and ticketing software, support services by third parties, e.g. software manufacturers and external service providers regarding third-party products, cleaners, security guards, auditors, transport of data carriers or the disposal of data carriers. However, the contractor is obliged to make appropriate and legally compliant contractual agreements to ensure the protection and security of the Customer's data, even in the case of externally contracted ancillary services.

9.5. The provisions of this clause 9 shall also apply if a subcontractor is engaged in a third country. The Customer hereby authorizes the Contractor, acting on behalf of the Customer, with a subcontractor who processes or uses the Customer data outside the EEA or Switzerland, including the EU standard contract clauses for the transmission of personal data to contract processors in third countries after the 5th of February 2010.

9.6. Insofar as the subcontractor is an international organisation or has its registered office in a third country, the provisions of GDPR Article 44 must be also complied, with respect to the data transmission to the respective subcontractor for the purpose of order processing in the subcontract. The Contractor is particularly aware that, in the absence of an adequacy decision pursuant to GDPR Article 45 (3) or the correct use of the EU standard contract clauses, such transmission is only permissible if the subcontractor has provided appropriate guarantees and if effective remedies are available, see GDPR Article 46. The Contractor is responsible for the required warranty measures in relation to the Customer. The Contractor is obliged to comply with the provisions of the GDPR Article 44 as well as the other provisions of the GDPR.

10. Term of this Agreement/Termination

10.1. The term and termination of this Agreement shall be governed by the terms of the "Term and termination of the service" Supply Agreement. A termination of the service agreement automatically results in a termination of this Agreement. An isolated termination of this Agreement is excluded. A termination for important reasons remains unaffected.

10.2. Notice of termination must be given in writing in order to be effective.

11. Additional Services

Clauses 1 to 8 shall apply accordingly if other bodies acting as agents carry out inspection or maintenance of automated procedures or data processing systems and if access to personal data cannot be excluded in the course of these works.

12. Data Protecting Control

12.1. The Contractor undertakes to grant access during normal business hours to The Customer's Data Protection Officer to carry out his/her statutory duties in accordance with clause 6 (4) of this Agreement.

12.2. The Contractor shall be obliged to make available to the Customer all necessary information to demonstrate the compliance with the obligations laid down in Article 28 (3) of the GDPR and to carry out checks which oblige the Customer or any other party to maintain confidentiality In accordance with the clause 6 (4) of this Agreement. The Contractor is obliged, upon appropriate request to demonstrate compliance with his duty to maintain confidentiality.

13. Liability

13.1. The Contractor is liable according to the legal liability regulations for damages of the Customer due to culpable breaches of the Contractor against this contract as well as against the legal data protection obligations that directly affect him. Insofar as third parties assert claims against the Customer which are caused by a culpable breach by the Contractor of this contract or by a statutory data protection obligation that directly affects him, the Contractor indemnifies the Customer from these claims upon first request. The liability of the Contractor under this Agreement shall be subject to the disclaimers and limitations set out in the Service Agreement.

13.2. Insofar as third parties assert claims against the Contractor that are caused by a culpable breach by the Customer of this Agreement or one of its duties as data controller, the Customer indemnifies the Contractor against these claims upon first request.

13.3. The Contractor undertakes to exempt the Customer from all possible fines imposed on the Customer on the first request to the extent that the Contractor bears responsibility for the infringement sanctioned by the fine.

13.4. The Customer also undertakes to exempt the Contractor from all possible fines imposed on the Contractor to the extent required on the first request, in which the Customer bears a share of the responsibility for the infringement sanctioned by the fine.

14. Court of Jurisdiction / Applicable Law

14.1. The parties of this Agreement shall submit to the jurisdiction of the courts of Stuttgart, Germany.

14.2. This Agreement shall be governed by and interpreted in accordance with the Laws of the Federal Republic of Germany to the exclusion of private international law.

15. Final Provisions

15.1. Changes and additions to this Agreement and all of its components - including any warranties of the Contractor - require a written agreement and the explicit reference to the fact that they constitute amendments or supplements to these terms. This also applies to waiving the requirement for making such changes in writing.

15.2. If any provision of this Agreement or the application thereof is held invalid, the invalidity shall not affect other provisions or applications of the Agreement which can be given effect without the invalid provisions or applications and to this end the provisions of this Agreement are declared to be severable. In this case, the contracting parties undertake to replace the ineffective provision with an effective one that comes closest to the economic purpose of the invalid provision. The same applies to any gaps in the Agreements.

15.3. Annex 1 "List of Customer Contacts for Data Processing", Annex 2 "Technical and Organisational Measures" and Annex 3 "List of Subcontractors" are part of this agreement.

. . . . .	. . . . .
Date, place	Date, place
. . . . .	. . . . .
(Signature Customer)	(Signature Onventis GmbH)
. . . . .	. . . . .
Name, First name, position	Name, First name, position

Annex 1
List of Customer Contacts for Data Processing

Clause 4 (6), Clause 7 (3) and Clause 9 (2) of the Data Processing Agreement refer to the practical implementation of the information requirements of the Contractor on this Annex..

	Name	Position	E-mail Addres	Phone Number
Date Protection Contact::				

Annex 2
Technical and Organisational Measures
according to GDPR Art. 32

§ 1 Subject

In order to ensure the security of the processing (Art. 32 GDPR), the Contractor assures the Customer of the existence of the following technical and organisational measures.

§ 2 General organisational measures

a. The Contractor has appointed as Data Protection Officer:
Dr. Ralf W. Schadowski, ADDAG GmbH, Krefelder Street 121, 52070 Aachen,
privacy@onventis.de

b. The contractor has the following regulations on data protection and confidentiality:
The contractor's employees are obliged to observe data protection and confidentiality. The designated documents may be inspected upon request at the contractor's premises.

c. The contractor has the following certifications in the areas of information technology, data protection and data security:
Onventis is a holder of certificate IS 693008 applying an information security system according to ISO/IEC 27001:2013 for the following scope:
- Consulting & Project Management for the implementation of the Onventis Open Procurement Network solution for customers.
- Customer support
- Cloud platform operation

The certificate can be presented at the request of the Customer.

§ 3 Confidentiality (Art. 32 paragraph 1 GDPR)

a. Access control
Unauthorised persons shall be denied access to data processing equipment as follows:
- Alarm system
- Access control system
- Security locks
- Locking system with chip card
- Identity check
- Determination of authorised persons
- Window sealing
- Cleaning and maintenance personnel committed to data protection
- Supervision of cleaning and maintenance
- Security guards
- Video surveillance

- Key regulation
- Locking system with transponder
- Manual locking system
- Duty of identification
- Logging of access
- Subdivision into safety zones
- Burglar-proof windows
- Fixed cleaning times
- Device and housing sealing

b. Access control

Unauthorised use of the data processing systems is prevented by the following measures:

- User account for each employee
- Authentication via directory services
- Virus protection solutions
- Packet Filter Firewall
- Dedicated networks for sensitive systems
- Authentication with password
- Single Sign On
- Access restriction according to end device
- Lock BIOS
- Intrusion Detection System
- Application Layer Firewall
- Arrangements in the event of staff leaving

c. Access control

Only authorised personnel can process and use the personal data released to them, while unauthorised persons can neither read nor change this data. The following measures are taken for this purpose:

- Documented authorisation concept
- Role concept
- Differentiated authorisations for different transactions/functions
- Strict password guidelines
- Keeping record of the login processes
- Automatic logout procedures
- Distribution of administrator rights among different persons
- Secure storage of (removable) data carriers
- System-side authorisation concept
- Differentiated authorisations for data objects
- Regular password changes
- Logging of data access
- Account blocking after multiple incorrect password entries
- Allocation of administrator rights to a minimum number of persons
- Keeping a record of deletion processes

d. Separation control

The guarantee of separate processing of data collected for different purposes is ensured by the following measures:

- Physically separate storage and processing
- Differentiated authorisations for data management
- Logical customer separation
- Attribution of data sets according to the purpose of processing
- Separation of productive and test systems
- Differentiation of administrative tasks in data management
- Documentation of the clients and associated data areas

e. Pseudonymisation

Personal data are processed in such way that they can no longer be assigned to a specific data subject without the addition of additional information unless a personal reference is absolutely necessary. This additional information is stored separately and it is subject to appropriate technical and organisational measures.

§ 4 Integrity (Art. 32 paragraph 1 GDPR)

a. Transfer control

During electronic transmission or transport, personal data cannot be read, copied, altered, or removed and the recipient of the data is known at all times, as the following measures are taken:

- Data communication via VPN tunnel
- Logging of the transmission processes
- Remote deletion from mobile devices
- Transport-encrypted data transmission (secure transmission on the Internet)
- Documentation of the transfer processes for physical transport

b. Input control

The control of the entry, modification and removal or deletion of personal data is implemented through the following measures:

- Working with individual user IDs
- Logging of all administrator activities
- Logging of the data changes
- Logging of access attempts
- Authorisation concept with separate input, modification and deletion powers
- Data collection instructions
- Plausibility checks
- User recognition-related logging
- Logging of the data entries
- Logging of data deletions
- Logging of failed access attempts
- Securing the log data against change and loss

§ 5 Availability and resilience

a. Availability control

The data processed is protected against accidental destruction or loss by the following measures:

- Backup and recovery concept
- Defined responsibilities for data backup
- Emergency plan
- Redundant IT systems
- Uninterruptible power supply
- Air conditioning in server rooms
- Fire and smoke detection systems
- Automatic notification system
- Protection against water ingress and flooding
- Keeping the backup in another fire compartment
- Regular test of data recovery
- Data carrier mirroring (RAID)
- Virtualised infrastructure
- Surge protection
- Climate monitoring (room temperature, humidity) in server rooms
- Fire extinguisher / automatic extinguishing system
- Automatic emergency call system
- Proof of the suitability of the premises and building structure

b. Rapid recoverability

All PSP instances are virtual and can be restored within minutes except in the case of catastrophic hardware failure. In this case, recovery is only possible with the purchase of new ESX hardware.

§ 6 Procedures for regular review, assessment and evaluation

a. Data protection management

A Data Protection Officer is not a subject to directives and reports directly and immediately to the management. The task of the Data Protection Officer is to ensure compliance with the German Federal Data Protection Act (BDSG) as well as the European Data Protection Regulation (GDPR) as well as other regulations on data protection in Onventis.

The Contractor has appointed an external data protection officer to perform the tasks pursuant to Art. 39 GDPR:

- Monitoring compliance with the GDPR, other Union or Member State data protection legislation including the personal data protection policies of the controller or processor.
- Training or regular awareness raising of the persons at Onventis who are active in the processing of personal data, with the provisions of the GDPR, the GDPR as well as other regulations on data protection.
- Supports the Contractor in the event of reported data protection incidents so that the relevant responsible parties are informed without delay. In the event of data protection incidents that result in a risk to the rights and freedoms of natural persons, supports the Contractor in informing the competent supervisory authority.

- Support in ensuring the rights of data subjects in accordance with the GDPR and responding to requests from data subjects in accordance with the prescribed process of running the data protection management system.

b. Order control

The assurance of commissioned data processing in accordance with the client's instructions is achieved through the following measures:

- Obligation of employees to maintain data secrecy
- Toleration and support of audits by the client
- Contractual penalties agreed
- Destruction of data after completion of the order
- Return procedure for documents that are no longer required
- Appointment of a company data protection officer
- Documentation and information about existing IT infrastructure
- Effective control rights for the client agreed
- Selection of subcontractor under due diligence aspects
- Review of the security measures taken by the subcontractor
- Ongoing review of the subcontractor and its activities

§ 7 Duty to inform

- If the application of the aforementioned measures is temporarily impossible for more than 4 hours or completely impossible, the contractor shall inform the client on working days within 72 hours.