Seatti

Contract on processing personal data according to EU General Data Protection Regulation

(AV Contract) according to Art. 28 DSGVO

Contract for the commissioned processing of personal data

between	and
	Seatti GmbH
represented by	*represented by*
	Johannes Eppler *Chief Product Officer Seatti* *johannes@seatti.co*
hereinafter: **Client**	hereinafter: **Contractor**

1. Introduction, scope, definitions

(1) This Agreement governs the rights and obligations of the Client and the Recipient (hereinafter referred to as the "Parties") in the context of processing personal data on behalf of the Client.

(2) This Agreement shall apply to all activities in which employees of the Contractor or subcontractors engaged by the Contractor (subcontractors) process personal data of the Client on behalf of the Client.

(3) Terms used in this contract are to be understood according to their definition in the EU General Data Protection Regulation. In this sense, the client is the "responsible party" and the contractor is the "processor". Insofar as declarations in the following are to be made "in writing", the written form according to § 126 BGB is meant. Otherwise, declarations may also be made in another form, provided that appropriate verifiability is ensured.

2. Subject and duration of processing

2.1. Subject

The Contractor is a provider of software for the management of hybrid workspaces, which is used by the Customer as a cloud-based SaaS service. The parties have concluded a contract for the use of the software.

The processing is based on the service contract existing between the Parties (hereinafter "Main Contract").

2.2. Duration

Processing shall commence on the signing date of the Main Contract and shall continue indefinitely until termination of this Agreement or the Master Agreement by either party.

3. Type, purpose and data subjects of the data processing:

3.1. Type of processing

Personal data in the sense of the GDPR are directly processed by the contractor in the form of a pseudonymized user-id. However, access to other personal data cannot be excluded. Specifically, IT, support and project management tasks may involve activities such as:

- Creation or modification of system users via admin client (direct editing of table) incl. assignment of roles, domains and groups according to client's specifications
- Review of log files or database tables in the event of malfunctions or preventive maintenance, which may contain personal data of system users
- Working with individual assets in the event of a malfunction (support request), which may contain personal information, depending on how the client uses them

The processing and use of the data shall take place exclusively in a member state of the European Union or in another state party to the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the client and may only take place if the special requirements of Art. 44 et seq. DSGVO are fulfilled. Data processing agreements are concluded with US service providers who are in a subcontracting relationship as defined in paragraph 7, to supplement standard contractual clauses which continue to apply. This also applies if their data processing services take place exclusively within EU territory.

3.2. Purpose of processing

The more detailed purpose of the processing is regulated in the service description of the main contract.

3.3. Type of data

The following data will be processed:

- Microsoft Company ID (pseudonymized)
- Microsoft User ID (pseudonymized)
- Input workspace booking data

In principle, access to personal data of system users (login information such as first name, last name, login name, email address, and at the request of the client also title, gender and language) cannot be excluded when carrying out the procedures listed in paragraph 3.1. However, personal data points beyond the pseudonymized MS User-ID will never be visible in plain text in processed log-files or database tables.

3.4. Categories of data subjects

Affected by the processing are:

- Seatti Services system users
- Employees of the client

4. Duties of the contractor

(1) The Contractor shall process personal data exclusively as contractually agreed or as instructed by the Client, unless the Contractor is legally obliged to carry out a specific processing. If such obligations exist for the Contractor, the Contractor shall notify the Client of these prior to processing, unless the notification is prohibited by law. Furthermore, the Contractor shall not use the data provided for processing for any other purposes, in particular not for its own purposes.

(2) The Contractor confirms that it is aware of the relevant general data protection regulations. It shall observe the principles of proper data processing.

(3) The Contractor undertakes to strictly maintain confidentiality during processing.

(4) Persons who may gain knowledge of the data processed in the order shall undertake in writing to maintain confidentiality, insofar as they are not already subject to a relevant confidentiality obligation by law.

(5) The Contractor warrants that the persons employed by it for processing have been familiarized with the relevant provisions of data protection and this Agreement prior to the start of processing. Corresponding training and awareness-raising measures shall be repeated on an appropriate regular basis. The Contractor shall ensure that persons deployed for commissioned processing are appropriately instructed and monitored on an ongoing basis with regard to compliance with data protection requirements.

(6) In connection with the commissioned processing, the Contractor shall support the Customer to the extent necessary in fulfilling its obligations under data protection law, in particular in creating and updating the list of processing activities, in carrying out the data protection impact assessment and any necessary consultation with the supervisory authority. The required information and documentation shall be kept available and provided to the Customer without undue delay upon request.

(7) If the Client is subject to inspection by supervisory authorities or other bodies or if data subjects assert rights against it, the Contractor undertakes to support the Client to the extent necessary, insofar as the processing under the contract is affected.

(8) The Contractor may only provide information to third parties or the person concerned with the prior consent of the Client. The Contractor shall immediately forward any inquiries addressed directly to it to the Client.

(9) To the extent required by law, the Contractor shall appoint a competent and reliable person as data protection officer. It must be ensured that there are no conflicts of interest for the commissioner. In cases of doubt, the Customer may contact the data protection officer directly. The Contractor shall inform the Customer without delay of the contact details of the data protection officer or give reasons why no officer has been appointed. The Contractor shall inform the Customer without delay of any changes in the person or the internal tasks of the data protection officer.

(10) As a matter of principle, the commissioned processing shall take place within the EU or the EEA. Any relocation to a third country may only take place with the consent of the client and under the conditions contained in Chapter V of the General Data Protection Regulation and in compliance with the provisions of this contract.

5. Processing safety

(1) The Technical and Organizational Measures described in Appendix 1 are defined as binding. They define the minimum owed by the Contractor. The description of the measures must be made in such detail that a knowledgeable third party can at any time undoubtedly recognize from the description alone what the minimum owed is to be. A reference to information which cannot be taken directly from this agreement or its appendices is not permissible.

(2) The Contractor shall establish security pursuant to Art. 28 Para. 3 lit. c, 32 DS-GVO, in particular in connection with Art. 5 Para. 1, Para. 2 DS-GVO. Overall, the measures to be taken are data security measures and to ensure a level of protection appropriate to the risk with regard to confidentiality, integrity, availability and the resilience of the systems. The state of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR must be taken into account.

(3) The data security measures may be adapted in accordance with the technical and organizational further development as long as the level agreed here is not undercut. The Contractor shall implement any changes required to maintain information security without delay. The Customer shall be notified of any changes without delay. Significant changes shall be agreed between the parties.

(4) Insofar as the security measures taken do not or no longer meet the requirements of the Customer, the Contractor shall notify the Customer without delay.

(5) Copies or duplicates shall not be made without the knowledge of the client. Technically necessary, temporary duplications are excepted, insofar as an impairment of the level of data protection agreed here is excluded.

(6) Dedicated data carriers originating from the Client or used for the Client shall be specially marked and shall be subject to ongoing management. They must be stored appropriately at all times and must not be accessible to unauthorized persons. Inputs and outputs are documented.

6. Rules for the correction, deletion and blocking of data

(1) The Contractor shall only correct, delete or block data processed within the scope of the order in accordance with the contractual agreement reached or in accordance with the Client's instructions.

7. Subcontracting relationships

(1) If and to the extent that the Contractor wishes to use subcontractors to provide the contractually agreed services and if it cannot be ruled out that these subcontractors have the possibility of obtaining knowledge of the Client's data in the course of their activities, the Contractor may only and only then commission the subcontractor and enable it to obtain knowledge of the Client's data if it has informed the Client specifically and in detail in text form about the points in item 6.2, has given the Client the opportunity to object (see item 7.3) and the Client has not raised an objection within the objection period. Subcontractors who are already in a subcontracting relationship with Seatti at the time the contract is concluded are listed in Annex 2.

(2) The information of the Contractor according to item 7.1 must contain at least in concrete and detailed form:

a. the identity of the subcontractor,

b. The specific services to be provided by the subcontractor to the contractor; and

c. Subcontractor's warranties or representations that it will comply with the provisions of this Order accordingly.

(3) The Customer shall be entitled to object to the assignment of a subcontractor in text form within 14 days after receipt of the information pursuant to Section 7.2, provided that this is not done arbitrarily.

(4) If and to the extent that data of the Customer becomes accessible to the subcontractor, the Contractor shall be obliged to agree in writing with the subcontractor, prior to the first making accessible of data of the Contractor, on a contract processing agreement imposing corresponding obligations on the subcontractor as regulated in this Agreement. Upon request of the Customer, the Contractor shall provide a copy of the order processing agreement and evidence of the Subcontractor's compliance with the obligations resulting therefrom. The Contractor shall ensure by agreement with its subcontractor that it is entitled to disclose this information to the Customer and that the Customer may also exercise its control rights pursuant to 7. directly against the subcontractor.

(5) Notwithstanding the provisions of Clauses 7.1-7.5, the Contractor shall be fully responsible for the Subcontractor and shall be liable for the Subcontractor's compliance with its obligations towards the Client.

(6) Not to be understood as a subcontracting relationship within the meaning of this provision are those services which the Contractor uses from third parties as an ancillary service to support the

execution of the order. These include, for example, telecommunications services, provision of data center infrastructure, maintenance and user service, cleaners, auditors or the disposal of data carriers. However, the Contractor shall be obligated to enter into appropriate and legally compliant contractual agreements and to take control measures to ensure the protection and security of the Customer's data, even in the case of externally contracted ancillary services.

8. Rights and obligations of the client

(7) The client alone is responsible for assessing the permissibility of the commissioned processing and for safeguarding the rights of data subjects.

(8) The client shall issue all orders, partial orders or instructions in documented form. In urgent cases, instructions may be issued verbally. The client shall confirm such instructions immediately in a documented manner.

(9) The Customer shall inform the Contractor without undue delay if it detects any errors or irregularities in the examination of the results of the order.

(10) The Customer shall be entitled to monitor the Contractor's compliance with the provisions on data protection and the contractual agreements to a reasonable extent itself or through third parties, in particular by obtaining information and inspecting the stored data and the data processing programs as well as other on-site checks. The persons entrusted with the control shall be granted access and inspection by the Contractor to the extent necessary. The Contractor shall be obliged to provide the necessary information, to demonstrate processes and to provide evidence required to carry out a control. The Contractor shall be entitled to refuse inspections by third parties if they are in a competitive relationship with the Contractor or if there are similar weighty reasons.

(11) Inspections of the Contractor shall be carried out without avoidable disruption to its business operations. Unless otherwise indicated for urgent reasons to be documented by the Customer, inspections shall take place after reasonable advance notice and during the Contractor's business hours, and not more frequently than every 12 months. Insofar as the Contractor provides evidence of the correct implementation of the agreed data protection obligations as provided for in Chapter 5 (8) of this Agreement, any checks shall be limited to random samples.

9. Notification requirements

(1) The Contractor shall notify the Client without delay of any violations of the protection of personal data processed on behalf of the Contractor. Reasonable suspicions thereof shall also be notified. The notification shall be sent to an address specified by the Customer within 24 hours of the Contractor becoming aware of the relevant event. It must contain at least the following information:

a. A description of the nature of the personal data breach, including, to the extent possible, the categories and approximate number of individuals affected, the categories affected, and the approximate number of personal data records affected;

b. the name and contact details of the data protection officer or other point of contact for further information;

c. a description of the likely consequences of the personal data breach;

d. A description of the measures taken or proposed by the Contractor to address the personal data breach and, if applicable, measures to mitigate its potential adverse effects

(2) Significant disruptions in the execution of the order as well as violations by the Contractor or the persons employed by the Contractor of the provisions of data protection law or the stipulations made in this contract shall also be reported immediately.

(3) The Contractor shall inform the Client without undue delay of inspections or measures by supervisory authorities or other third parties, insofar as these relate to the commissioned processing.

(4) The Contractor warrants to support the Client in its obligations pursuant to Art. 33 and 34 of the General Data Protection Regulation to the extent necessary.

10. Instructions

(1) Within the scope of the order description agreed in this agreement, the Customer reserves a comprehensive right to issue instructions regarding the type, scope and procedure of data processing, which it may specify by means of individual instructions. Changes to the object of processing and changes to procedures must be jointly agreed and documented. The Contractor may only provide information to third parties or the data subject with the prior written consent of the Client.

(2) The Client shall immediately confirm verbal instructions in text form. The Contractor shall not use the data for any other purposes and shall in particular not be entitled to pass them on to third parties.

(3) The Contractor shall inform the Customer without delay if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Customer.

11. Termination of the order

(1) If, upon termination of the contractual relationship, data processed in the order or copies thereof are still in the Contractor's power of disposal, the Contractor shall, at the Client's option, either destroy the data or hand them over to the Client. The Client shall make this choice within 35 Days of being requested to do so by the Contractor. The destruction shall be carried out in such a way that a recovery even of residual information is no longer possible with reasonable effort.

(2) The Contractor shall provide proof of proper destruction and submit it to the Client without delay.

(3) Documentation serving as proof of proper data processing shall be kept by the Contractor at least until the end of the third calendar year after the end of the contract. The Contractor may hand them over to the Client for the purpose of discharging the Contractor.

12. Liability

(1) For compensation of damages suffered by a person due to unauthorized or incorrect data processing within the scope of the contractual relationship, the Client and the Contractor shall be jointly and severally liable to the person, whereby the liability for damages shall be borne between the Client and the Contractor in proportion to their respective fault.

(2) The Contractor shall bear the burden of proof that any damage is not the result of a circumstance for which it is responsible, insofar as the relevant data was processed by it under this Agreement. As long as this proof has not been provided, the Contractor shall indemnify the Customer upon first request against all claims asserted against the Customer in connection with the commissioned processing. Under these conditions, the Contractor shall also reimburse the Client for all legal defense costs incurred.

(3) The Contractor shall be liable to the Client for any damage culpably caused by the Contractor, its employees or the subcontractors engaged by it to perform the contract or the subcontractors engaged by it in connection with the provision of the contractual service commissioned.

(4) Numbers (2) and (3) shall not apply insofar as the damage was caused by the correct implementation of the commissioned service or an instruction issued by the Client.

Signatures

9/7/2023Place, date

Place, date

Client

Contractor

Annex 1 - Technical and Organizational Measures

The technical and organizational measures (TOMs) described below apply to all standard service offerings provided by Seatti GmbH (hereinafter "Seatti"), unless the customer is responsible for the security and data protection TOMs. The measures described are based in particular on Art. 28 (3) lit. c & Art. 32 DSGVO as well as Chapter 3 (Technical and Organizational Measures) and Chapter 5 (Quality Assurance and Other Obligations of the Contractor) of this Agreement, which pick up the requirements of the DSGVO. The structure of the measures is based on the proposal of the authorities and is derived directly from the requirements of Art. 32 DSGVO. These are subdivided into measures for ensuring the

- Confidentiality
- Integrity
- Availability and resilience
- Regular review, assessment and evaluation

Risk identification

Seatti implements the Privacy by Design principle from the very beginning. The design of processes and systems is based in particular on the principles of pseudonymization and minimization. Data is only collected to the minimum extent and level of detail necessary for the provision of the specific service.

The usage data (workspace bookings) of the Seatti Services are only stored and processed in connection with a pseudonymized user ID. An assignment of personal data takes place exclusively within the client systems and is not visible to Seatti. Input data from workspace planning is only linked to this user ID and does not provide any further information about personal data.

The service is provided as cloud-hosted software. Any physical infrastructure for data processing is physically outsourced to a Premium Cloud subcontractor within the meaning of Annex 2. In each case, it is ensured that the data storage takes place in the territory of the EU and used servers are stationed accordingly. Our Cloud subcontractor guarantees in its Data Processing Addendum (DPA) that only the selected server region is used for data processing unless actively initiated otherwise by the client. The DPA also serves as a GDPR-compliant supplement to the standard contractual clauses for cooperation with US service providers and corresponds to current recommendations of ECJ case law in order to ensure the maximum possible protection of data even after the suspension of the US Privacy Shield by the ECJ. The physical processing as well as storage of the data continues to take place exclusively on Servers at a server location in Europe. Dedicated Azure Cosmos Database are deployed in a dedicated Virtual Private Cloud (VPC) with dedicated firewalls. Access must be granted via IP access list or VPC peering. All network traffic is encrypted using SSL/TLS.

Seatti employees function completely remotely Since personal data is never stored on local endpoints or directly viewable, unauthorized physical intrusions pose a low risk.

All technical and organizational measures listed below are documented centrally and made available to all employees.

Confidentiality

1.1. *Entry control*

Seatti does not have its own physical facilities for storing or processing data. Data processing facilities are utilized by established third party vendors as previously described. No personal data is ever stored on any equipment other than that of the third party vendors. Therefore, physical access to terminal equipment or any other hardware under Seatti's jurisdiction is not relevant to the protection of Personal Data.

Azure as a data center offers extensive security measures for compliance with the GDPR. Several standards are implemented, including ISO 27001 for technical measures, ISO 27017 for cloud security, and ISO 27018 for cloud privacy. In the Azure GDPR DPA, Azure provides further assurances:

- Data is processed exclusively in the precisely instructed manner
- Azure maintains detailed technical and organizational measures
- In the event of security incidents, Azure customers are notified of incidents as soon as they become aware of them

Access control to Azure data centers and all other technical and organizational measures implemented by Azure are detailed at Physical security of Azure datacenters - Microsoft Azure

1.2. *Admission control*

Digital access to the storage media of personal data must generally be protected against unauthorized access by means of password-protected access and passwords are randomly generated by an encrypted password manager. Access data and passwords in particular must never be stored locally, but only in a SOC2-certified password management tool. Also, sharing of newly created login credentials or shared access is never done unencrypted via standard communication channels, but exclusively by means of the deployed password management software. In this way, user accesses are centrally managed, documented and their validity regularly checked. As a matter of principle, initial passwords must be changed immediately after they are received and stored in a personal password container in the certified password management tool. E-mails are only sent and read via the TLS-encrypted domain belonging to the company. In addition, screen workstations are automatically locked after two minutes and must be unlocked by re-authentication.

1.3. *Access control*

A minimum number of administrators required for operation, who can manage user access and roles, is intended to guarantee a minimum possible scope of access. In addition, dedicated user roles are created for different task profiles, with which individual users are granted only the minimum necessary usage and access authorizations. In general, no personal or confidential data is to be transferred or stored locally or in paper form. Access to databases and the entry, modification and deletion of data are logged using Microsoft azure Sevices Log and can only be viewed by administrators.

1.4. *Separation control*

Seatti Software is multi-client capable and all customer-related data is managed in a separate client in a central data processing system. Data records are provided with a client ID, which is used for authentication and clear demarcation. Clients can only view data authenticated for them in their user interface and, if necessary, edit it to the extent provided.

1.5. *Pseudonymization*

In principle, only the minimum data required to provide our services is collected (privacy by design). The stored data cannot be assigned to any natural person, since the only means of identification is a pseudonymized user ID. Assignment data that could allow a unique identification are exclusively managed by the client and / or its partners. Any transmission of data between these parties and Seatti is subject to TLS encryption. If data of any kind is transferred to other data processing systems for analysis purposes, it will be completely anonymized beforehand.

2. Integrity

2.1. *Transfer control*

Personal data should not leave the azure Cloud as a matter of principle. Even for analysis purposes, the data is evaluated in the cloud environment or completely anonymized before transfer. If a transfer is necessary, any transfer must be agreed in advance with the data protection officer, appropriate encryption measures must be taken and the transfer must be logged and documented.

2.2. *Input Control*

The processing of data is logged in the azure system log and can be viewed by the system administrators at any time. Only the designated system administrators are authorized to edit data. They only have access via individual logins, which means that logged activities can be clearly assigned to an editor. Further reading rights that go beyond the scope required for automated operation are only granted to the minimum extent necessary and after inspection by the data protection officer.

3. Availability and resilience

A centralized cloud backup plan including configured security policy guarantees regular and automated daily backups across all azure services and creates backup copies of all applications as well as snapshots of the databases used which are stored database instances fully separated from the production and testing instances. Logging and monitoring additionally allow regular verification of the backup. The electrical systems of Azure data center are designed to be fully redundant and equipped with an emergency power supply to be unaffected by outages around the clock.

4. Procedures for regular review, assessment and evaluation

4.1. *Data protection measures*

The measures listed here are reviewed annually, together with a data protection expert from an independent law firm, to ensure that they are up-to-date and effective. After each review, the TOMs are adjusted accordingly and all employees are informed of the adjustments. Data protection guidelines and TOMs are documented centrally and are accessible to all employees at all times. Likewise, the accesses of the system administrators and all other user accesses and their respective access authorizations are documented centrally and reviewed at least once a year.

4.2. *Incident Response Management*

Security incidents can be reported at any time by telephone or e-mail to the data protection officer (see 4.5 TOMs). He or she will immediately forward the report to the system administrators documented in accordance with 4.1 (TOMs) in order to initiate measures directly.

4.3. *Privacy-friendly default settings*

Data is only collected to the extent necessary for the respective purpose of providing our services. In addition, data is always stored pseudonymously and only linked to assignment data in client systems.

4.4. *Order control*

Subcontractors within the meaning of Chapter 6 of the AV shall only be permitted to process data after signing an AV and reviewing the technical and organizational measures of the respective contractor. Another requirement is to ensure that the contractor has an accessible data protection officer. Furthermore, after completion of an order, it is ensured that all previously transferred data is completely deleted.

4.5. *Data Protection Officer*

The Data Protection Officer for Seatti GmbH:

heyData GmbH,
Schützenstraße 5,
10117 Berlin,
+498941325320,
datenschutz@heydata.eu , Amtsgericht Berlin-Charlottenburg.

Annex 2 – Subcontractors

Name of the Provider	Services Provided	Location of the Servers
Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Provision of data center infrastructure Hosting, E-Mails	EU (Germany, Ireland and Netherlands)
Tableau Salesforce.com Germany GmbH, Erika-Mann-Str. 31, 80636 München, Deutschland	Data Analysis and reporting to optimize internal processes and Customer service (processing pseudonymized data)	EU

Subcontractor 1: Microsoft Azure

The subcontractor's warranties are based on the Azure GDPR Data Processing Addendum and the standard contractual clauses contained therein, pending further legal safeguards to protect the transfer of data overseas.

For all services used by Azure, the server location will be in Europe exclusively.Auswählen der richtigen Azure-Region | Microsoft Azure

Subcontractor 2: Salesforce Tableau

The subcontractor's warranties are based on the Salesforces Data Processing Addendum.

Salesforce complies with security standards, controls, and requirements such as ISO 27001:2013, PCI DDS, GDPR (Privacy Shield) , SOC 2, and HIPAA and Others See Salesforce Compliance Portal