Contract For Data Processing Agreement

according to Art. 28 GDPR for SmartStash

Between

- Responsible -
hereinafter referred to as **client**

And

Fellowmind Germany GmbH
Technologiepark 8
33100 Paderborn

- Processor -
hereinafter referred to as **contractor**

collectively also hereinafter referred to as the **"Parties".**

Fellowmind

Preambel

This contract for order processing regulates the rights and obligations with regard to the instruction-bound data processing of the parties within the scope of the service provision by the contractor. The client has carefully selected the contractor and in particular ensured that the contractor offers sufficient guarantees that suitable technical and organizational measures are carried out in such a way that the processing of personal data is carried out by him in accordance with the data protection regulations applicable to him and the protection of the Rights of the persons affected by the processing are guaranteed.

1. Subject And Duration Of The Assignment

1.1. Object
The subject of the order for data handling is the performance of the following tasks by the contractor:

The contractor installs the SmartStash front-end software in the client's Microsoft 365 environment and sets up the software according to the client's wishes. The front end is linked via Azure to the back end, which is located in the client's Azure cloud.

1.2. Place of processing by the contractor
The provision of the contractually agreed data processing takes place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area (EEA).

1.3. Duration
The order is granted for an unlimited period and can be terminated by either party with a notice period of 3 months to the end of the year.

1.4. The client can terminate this contract and the underlying legal relationship according to Section 1.1 at any time without notice if the contractor has seriously violated data protection regulations or the provisions of this contract, the contractor cannot or does not want to carry out an instruction from the client or the contractor has control rights of the client refused in breach of contract. In particular, non-compliance with the obligations agreed in this contract and derived from Art. 28 GDPR constitutes a serious violation. In the case of simple – i.e. neither intentional nor grossly negligent – violations, the client shall set the contractor a reasonable period within which the contractor can remedy the violation.

1.5. The commissioning of the contractor does not release the client from his obligation to comply with the data protection regulations applicable to him, in particular with regard to the legality of the processing and the

protection of the rights of the persons concerned (Art. 12 to 22 GDPR). Against this background, the client remains responsible for data processing within the meaning of Art. 4 No. 7 GDPR.

2. Specification Of The Contract

2.1. Type of intended processing in accordance with Art. 4 No. 2 GDPR

The following types of processing are provided for in the context of order processing:

- Capture
- Storage
- Adaption or Change
- Reading
- Query
- Use For Operations
- Restriction
- Delete

2.2 Purpose of the intended processing of data

Processing of personal data of the client takes place for the following reasons:

- Explicit order from the client, e.g. setting up new users or authorizations
- Operation of the client's systems (maintenance, troubleshooting or implementation of change requests)
- Storage of personal data in order to establish a clear link between the activity and the assignee
- Storage of personal data as a contact to enable communication via electronic channels, e.g. email, chat, video conference and telephone call.
- Storage of personal data in order to be able to allocate offers, orders, order confirmations and invoices to an agent.
- Storage of personal data in the accounting system in order to be able to carry out transfers and allocate invoices.

2.3. Type of personal data

The subject of the processing of personal data is the following data types/categories:

(Note: Please delete what is not applicable or add further positions)

- Personal master data
- Communication data (e.g. telephone, email)
- Contract master data (contractual relationship, product or contract interest)
- Customer history

- Contract billing and payment data

2.4. Categories of data subjects

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:
- Customers
- Employees (of the customer)
- Suppliers

3. Authority Of The Client

3.1 Der contractor and any person authorized by him to process personal data may only process the data processed on behalf of the client in accordance with documented instructions. Processing for purposes other than those set out in this contract is not permitted.

The authorized persons of the client are to be explicitly named to the contractor in writing after the order has been placed (full name, organizational unit, contact details). In the event of a change or a long-term prevention of the named persons, the contractual partner must be informed immediately of the successor or representative, at least in text form.

3.2 The instructions of the client are initially defined by this contract and can be changed, supplemented or replaced by individual instructions (individual instructions). The client is entitled to issue corresponding instructions at any time. The individual instructions must be documented by the client and the contractor.

3.3 If the contractor is of the opinion that instructions violate applicable law, he will inform the client of this immediately. In this case, the contractor is entitled to suspend the implementation of the instruction until it has been confirmed or changed by the client. Processing that deviates from the instructions of the client is only permitted if the contractor is obliged to do so by the law of the Union or the member states to which the contractor is subject. In such a case, the contractor shall notify the client of those legal requirements prior to processing, unless the law in question prohibits such notification because of an important public interest.

4. Commitment To Confidentiality

When data is processed by the contractor, its employees are prohibited from collecting, processing or using personal data without authorisation. The contractor will obligate all persons entrusted by him with the

processing and fulfillment of this contract accordingly (obligation of confidentiality, Art. 28 Para. 3 lit. b DSGVO) and ensure compliance with this obligation with due care. These obligations must be drafted in such a way that they continue even after the termination of this contract or the employment relationship between the employee and the contractor. Evidence of the obligations must be provided to the client in a suitable manner upon request.

5. Technical And Organizational Measures (TOM)

5.1   The contractor has designed his internal organization in such a way that all special data protection requirements to be observed by him as a processor are observed.

5.2   In this context, he has taken the technical and organizational measures specified in Annex 1 in accordance with Art. 28 (3) lit. c, 32 GDPR, which are necessary to ensure the requirements for security of processing. Taking into account the type of processing and the information available to him, the contractor will support the client as best as possible in complying with the technical and organizational measures to be taken by the client and his obligations under Art. 32 GDPR.

5.3   The contractor has given the client a list of the technical and organizational measures he has taken before the conclusion of this contract for examination.

5.4   The technical and organizational measures taken by the contractor are subject to technical progress and further development. Against this background, the contractor is permitted to use new technologies or technical tools with which the protection of the personal data processed by him can be improved. In any case, the safety level of the measures stipulated in this contract must not be undercut.

5.5   The contractor will document significant changes and present them to the client in this context without being asked in a correspondingly adapted annex.

5.6   Upon request, the contractor shall provide suitable evidence that he has implemented all the necessary technical and organizational measures. To prove the technical and organizational measures taken, the contractor can present current attestations, reports or report excerpts from independent bodies (e.g. auditors, auditors, data protection officers, IT security department, data protection auditors, quality auditors) or suitable certification (e.g. according to Art. 42 DSGVO) by an IT - Submit a security or data protection audit (e.g. according to BSI basic protection).

5.7 The contractor does not use the personal data provided for processing for any other purposes, especially not for its own purposes. Copies or duplicates (including backups) of the personal data are not created without the knowledge of the client.

5.8 In the area of order-related processing of personal data, the contractor warrants that all agreed measures will be carried out in accordance with the contract. He assures that the data processed for the client will be strictly separated from other databases.

6. Contractor's Obligations

6.1 The contractor ensures that a register of processing activities is properly maintained in accordance with the requirements of Art. 30 (2) GDPR.

The contractor must contribute to the appropriate extent to the creation and updating of the list of processing activities by the client. He must provide the client with the information required in each case in a suitable manner.

6.2 The contractor will inform the client immediately if he is of the opinion that this contract or parts thereof do not meet the requirements for a contract for order processing according to the relevant provisions of the GDPR and/or any guidelines, recommendations or other opinions of the supervisory authorities, in particular the Data Protection Conference, which corresponds to the former Art. 29 Data Protection Group or the European Data Protection Board. In such a case, the parties will work together to make the necessary adjustments to this contract.

6.3 The Contractor shall inform the Client immediately if the Client's data at the Contractor is endangered by attachment or confiscation, insolvency or composition proceedings or by other events or measures by third parties. The contractor will immediately inform everyone involved in this context that the sovereignty and ownership of the data lies exclusively with the client as the person responsible within the meaning of the GDPR.

6.4 In the event of disruptions, suspected data protection violations or violations of contractual obligations by the contractor, suspected security-related incidents or other irregularities in the processing of personal data by the contractor, by persons employed by him within the scope of the order or by third parties, the contractor will notify the client immediately in writing or in text form. The same applies to examinations of the contractor by the data protection supervisory authority. The notification of a personal data breach shall contain at least the following information:

- A description of the nature of the personal data breach, including, where possible, the categories and number of data subjects affected, the categories affected and the number of personal data sets affected;
- A description of the actions taken or proposed by the contractor to remedy the breach and, where appropriate, actions to mitigate its possible adverse effects.

The contractor immediately takes the necessary measures to secure the data and to reduce possible adverse consequences for those affected, informs the client about this and requests further instructions.

The contractor is also obliged to provide the client with information at any time if his data is affected by an infringement under this paragraph.

6.5 To the extent required by law, the Contractor has appointed or will appoint a data protection officer who will perform the tasks incumbent on him pursuant to Art. 38, 39 GDPR. The contractor has communicated the contact details of the data protection officer to the data protection supervisory authority responsible for him. The client must be informed immediately of a change in the person of the company data protection officer/contact person for data protection or an initial appointment.

6.6 Insofar as the client is subject to an inspection by the data protection supervisory authority, administrative offense or criminal proceedings, the liability claim of a person concerned or a third party or another claim in connection with the order processing at the contractor, the contractor must support him to the best of his ability.

7. Subcontracting Relationships

7.1 Subcontracting relationships within the meaning of this provision are services that relate directly to the provision of the main service. This does not include ancillary services that the contractor z. B. as telecommunications services, mail/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the contractor is obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the client's data, even in the case of outsourced ancillary services.

7.2 The Contractor may only commission subcontractors (other processors) with the prior express written or documented consent of the Client. The client agrees to the commissioning of the subcontractors listed in Annex 2 under the following conditions:

Outsourcing to subcontractors is permitted if the contractor notifies the client of such outsourcing to subcontractors a reasonable time in advance in writing or in text form and the client does not object to the planned outsourcing in writing or in text form to the contractor by the time the data is handed over.

7.3   The transfer of the client's personal data to the subcontractor and his first action are only permitted if all the requirements for subcontracting are met.

7.4   If subcontractors are to be involved in a third country, the contractor must ensure that an appropriate level of data protection is guaranteed for the respective subcontractor (e.g. by concluding an agreement based on the EU standard data protection clauses). Upon request, the contractor will provide the client with evidence of the conclusion of the aforementioned agreements with its subcontractors.

7.5   Another outsourcing by the subcontractor

☐ is not permitted;
☒ requires the express consent of the main client (at least text form);
☐ requires the express consent of the main contractor (at least text form);

7.6   All contractual provisions in the contract chain are also to be imposed on the other subcontractor. The parties make it clear that the contractor is always liable to the client for compliance with the obligations of the subcontractor. In the event of a breach of the obligations arising from the agreement with the contractor or a breach of relevant legal requirements by the subcontractor, the contractor remains fully responsible to the client.

8. Support Obligations Of The Contractor

8.1   The contractor will support the client as best as possible in fulfilling his obligations to respond to requests to exercise the rights of the data subjects (in the sense of Art. 12-22 GDPR) with regard to their personal data.

The contractor will inform the client immediately, in particular about all requests for information, correction, deletion, restriction and data transfer from affected persons. The contractor will immediately forward corresponding applications and requests to the client. The contractor is not authorized to provide data subjects or third parties with information about the personal data processed in the order.

8.2   The contractor will support the client to the best of his ability in fulfilling his legal obligations under Art. 32 to 36 GDPR. Insofar as necessary, the contractor will therefore in this context in particular

- ensure an appropriate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing as well as the predicted probability and severity of a possible violation of the law through security gaps and enable relevant violation events to be identified immediately,
- the obligation to report breaches of personal data to the client without undue delay,
- support the client within the scope of his obligation to inform the persons concerned and make all relevant information available to him in this context without delay,
- support the client in carrying out a data protection impact assessment,
- assist the client in prior consultations with the supervisory authority.

8.3 The contractor will inform the client immediately about all control actions and measures of a data protection supervisory authority. This also applies if a competent authority investigates the processing of personal data by the contractor as part of administrative offense or criminal proceedings.

8.4 Insofar as the client is exposed to controls by the supervisory authorities, administrative offense or criminal proceedings, claims by a data subject pursuant to Art. 82 GDPR, claims by a third party or another claim in connection with the order processing at the contractor, the contractor will support the client in the best possible way.

8.5 The parties undertake to immediately remedy any defects found in the course of the inspection by the supervisory authorities and in connection with this contract.

9. Correction, Restriction And Deletion Of Data

9.1 The contractor will only correct or delete personal data of the client processed by him on his instructions. If data protection-compliant deletion or restriction of data processing is not possible, the client can commission the contractor with the data protection-compliant destruction of data carriers and other materials. If an affected person contacts the contractor directly for the purpose of correction or deletion of their personal data or information about their personal data, they will forward this request to the client without delay.

9.2 The contractor will return all documents, data and data carriers provided to the client after the end of the main contract or at any time at the request of the client, unless there is an obligation to store the personal data under Union law or the law of the Federal Republic of Germany - Clear. This also applies to any data backups by the contractor. The contractor must provide documented evidence of the proper deletion of any data that is still available. Documents and data carriers to be disposed of must be destroyed in accordance with DIN 66399.

9.3 The client has the right to control the complete and contractual return or deletion of the data at the contractor in an appropriate manner.

9.4 The contractor is obliged to treat confidentially the data that has become known to him in connection with the main contract even after the end of the main contract. The present agreement remains valid beyond the end of the main contract as long as the contractor has personal data that has been sent to him by the customer or that he has collected for him.

10. Client Control Rights

10.1 Before starting data processing, and then regularly thereafter, the client will ensure that the contractor's technical and organizational measures are in place. For this he can z. B. Obtaining information from the contractor, having existing attestations from experts, certifications or internal audits presented to him or the technical and organizational measures of the contractor himself personally checked after timely coordination during normal business hours or have them checked by a competent third party, provided that this is not in is in a competitive relationship with the contractor. The client will only carry out checks to the extent required and will not disturb the contractor's operational processes disproportionately.

10.2 The Contractor undertakes to provide the Client with all information and evidence required to carry out an inspection of the Contractor's technical and organizational measures within a reasonable period of time upon his verbal or written request.

10.3 The client documents the control result and informs the contractor about it. In the event of errors or irregularities that the customer finds, in particular when examining the results of the order, he must inform the contractor immediately. If facts are found during the check that require changes to the ordered procedure to avoid them in the future, the client will inform the contractor of the necessary changes to the procedure immediately.

11. Liability

The liability of the parties is based on the liability regulations of Art. 82 GDPR.

12. Final Provisions

12.1   The parties agree that the defense of the right of retention by the contractor i. s.d. § 273 german BGB with regard to the data to be processed and the associated data carrier is excluded.

12.2   Changes and additions to this contract must be in writing. This also applies to the waiver of this formal requirement. The priority of individual contractual agreements remains unaffected.

12.3   If individual provisions of this contract are or become invalid or unenforceable in whole or in part, this shall not affect the validity of the remaining provisions.

12.4   This contract is subject to the law of the Federal Republic of Germany. The place of jurisdiction is - as far as permissible - the registered office of the contractor.

Attachment 1
General technical and organizational measures

The annex describes the technical and organizational measures that ensure and provide evidence that the processing is carried out in accordance with Art. 24 GDPR. These result from Art. 32 Para. 1 GDPR. The contractor has implemented the following measures for this.

Protection goals	Measure	Implementation Of Measure
confidentiality **Art. 32 Abs. 1 lit. b) GDPR**	**Access Control** Unauthorized persons must be denied access to data processing systems with which personal data is processed. - Central reception and handover of visitors to their own employees.	- No free moving visitors. - Mass data systems behind lock. - Transponder key system with role-specific authorizations for defined areas. - Data center operation outsourced to other areas of the building with camera surveillance and separate access control. - access control - It must be prevented that data processing systems can be used by unauthorized persons. - Access via personalized transponder locking system. - Systemic access with rights and role concept via AD.
	Access Control It must be prevented that data processing systems can be used by unauthorized persons. - Access via personalized transponder locking system.	- Access via personalized transponder locking system. - Systemic access with rights and role concept via AD.

	Access Control It must be ensured that those authorized to use a data processing system can only access the data subject to their access authorization and that personal data cannot be read, copied, changed or removed without authorization during processing.	- Differentiation of the areas of responsibility in the job roles of the employees. This tightens the purpose limitation in relation to the personal data. - Use of system-side role separation in CRM and ERP system.
	Separation Control It must be ensured that data collected for different purposes can be processed separately.	- Functional areas linked to the job role in the data processing systems CRM, ERP and service entry system (RP).
Integrity **Art. 32 (1) b) GDPR**	**Disclosure Control** It must be ensured that personal data cannot be read, copied, changed or removed without authorization during electronic transmission or during their transport or storage on data carriers, and that it can be checked and determined to which bodies personal data is transmitted by institutions intended for data transmission.	- Data transmission and transport of personal customer data takes place exclusively after individual request and individual approval by the customer. - The transport is either digitally encrypted or physically accompanied by trained employees.
	Input Control It must be ensured that it can be subsequently checked and determined whether and by whom personal data has been entered, changed or removed in data processing.	- The standard mechanisms of the standard CRM and standard ERP are used for traceability.
Availability And Resilience **Article 32(1)(b) GDPR**	**Availability Control** It must be ensured that personal data is protected against accidental destruction or loss.	- Regular data backups are carried out in accordance with the data backup concept.

Recoverability **Art. 32 (1) c) GDPR**	**Measures For Rapid Recovery** In the event of an unforeseen incident, it must be ensured that the personal data can be used again "quickly" according to their purpose. - A certain redundancy is maintained in accordance with the disaster recovery concept.	- A certain redundancy is maintained in accordance with the disaster recovery concept.
Procedures for regular review, assessment and evaluation **Article 32 paragraph 1 letter d) GDPR**	**Order Control** It must be ensured that personal data processed in the order can only be processed in accordance with the instructions of the client.	- The appointed data protection officer ensures compliance and continuously optimizes to ensure sustainability.
	Privacy Management To protect personal data, it must be ensured that a data protection organization is established, and responsibilities are defined	- The data protection officer Ms. Spedt (ecoprotec GmbH, Pamplonastraße 19, 33106 Paderborn) and the management (represented by the managing director Mr. Scheibe) use organizational measures to ensure that data protection is actively monitored and observed and that further optimization is promoted.
Pseudonymization and encryption **Art. 32 Para. 1 lit. a) GDPR**	**Pseudonymization** The design of data processing must ensure that the risks to data subjects are minimized.	- The data processing takes place on a project basis. - - Non-project members generally do not have access. - - Pseudonymization takes place in individual cases through separate storage of plain data and keys.
	Encryption	- Access to the processing systems is encrypted.

	Access to the personal data is only to be granted to the authorized group of people.	- Administrators are instructed and obliged to their special role.

The technical and organizational measures described are not an exhaustive list. These and other measures serve to ensure data security and to ensure a level of protection appropriate to the risk with regard to the protection goals described in this annex. Furthermore, the measures are subject to technical progress and further development. The actual security level of the specified measures is not undercut.

Status: 08.01.2021 / MS

Attachment 2

List of existing subcontracting relationships within the framework of order processing (according to 7.2 of the contract)

Company	Address / Country	Contact Details	Description Of Services
Microsoft Ireland Operations Limited	Ireland One Microsoft Place South County Business Park Leopardstown Dublin 18 D18 P521		The Azure backend is in the EU Microsoft Cloud
Mailjet GmbH	Alt-Moabit 2, 10557 Berlin, Germany		Mail is sent by this external service

Attachment 3

The recipients of instructions from the contractor are:

Last Name, First Name	Organizational Unit	Phone	eMail
Scheibe, Michael	CFO	+49 5251-16192-0	michael.scheibe@fellowmind.de
Rossing, Gertjan	COO	+49 5251-16192-0	gertjan.rossing@fellowmind.de
Bracht, Andreas	CCO	+49 5251-16192-0	andreas.bracht@fellowmind.de