zavvy

Terms of Service

Preamble

Zavvy GmbH ("Zavvy," "we," "our," or "us") offers tools for employee enablement, onboarding, and learning & development as SaaS.
Zavvy and the customer (as defined in the paragraph below) may individually be referred to as a "party" and collectively "the parties."
The parties intend to establish the legal framework for the use of the Zavvy platform with this agreement for the provision of Software-as-a-Service (**"contract"**).

The contract is effective as of the date that you sign up for any service online or submit a service order that references this contract (the "**effective date**").
By accepting this contract, either by clicking a box indicating your acceptance, executing an order form or other document that references this contract, by using (or making any payment for) Zavvy services, or by otherwise indicating your acceptance of this contract, you: (1) agree to this contract on behalf of the customer indicated on the order (if applicable) or the organization, business, or other legal entity for which you act ("customer," "you," or "your"); and (2) represent and warrant that you have the authority to bind the customer to this contract. If you do not have such authority, or if you do not agree with this contract, you must not accept this contract and may not use Zavvy services.

Many organizations, such as businesses, use Zavvy's services. If you are accessing or using the service on behalf of an organization, then your organization is legally and financially responsible for your access to and use of the service as well as for the use of your Zavvy account by others affiliated with the organization, including any employees, agents or contractors. For the avoidance of doubt, the organization, company, or other legal entity for which you act will be considered the customer under this contract.

The following is contractually agreed between the parties:

1. Scope of Services

1.1 Zavvy shall provide the customer with the services outlined in this contract and agreed upon during the order process and managed in the subscription settings.

in the agreement conditions for the term of the contract in the Zavvy account.

1.2 Zavvy may use the assistance of third parties in the provision of all services covered by the contract and/or have the services provided in whole or in part by a third party.

1.3 The customer acknowledges that based on the current state of the art it is impossible to produce complex software products completely free of errors. Therefore, Zavvy does not owe the complete freedom from errors of the services and the underlying software, but only the freedom from such errors that limit their use in a significant way.

1.4 Zavvy is entitled, at its own discretion, to make the customer's access to and use of new functionalities of the services dependent on the conclusion of a separate agreement and the payment of an additional fee at any time.

2. **Usage Rights**

2.1 The services may only be used by the customer and only for the purposes agreed in the contract. During the term of the contract, the customer may access the services by means of telecommunications (via the Internet) and use the functionalities associated with the software by means of a browser in accordance with the contract. The customer shall not be granted any further rights, in particular to the services or the infrastructure services provided in the respective data center, if any. Any further use requires the prior written consent of Zavvy.

2.2 The customer can invite any number of users that are part of the customer's business to their Zavvy account. Pricing will dynamically be adapted to the number of users as set forth in 9.1.

2.3 The customer may not use the services beyond the agreed scope of use or allow third parties to use the services or make them available to third parties. In particular, the customer is not permitted to reproduce, sell or temporarily transfer, rent or lend the services or the software underlying the services or parts thereof.

2.4 Zavvy shall be entitled to take reasonable technical measures to protect against any use not in accordance with the contract. The contractual use of the services may not be impaired thereby more than only insignificantly.

2.5 In case of an exceeding of the scope of use by the customer or a user contrary to the contract or in case of an unauthorized transfer of use, the customer shall immediately provide Zavvy upon request with all information available to him for the assertion of claims due to the use contrary to the contract, in particular name and address of the user.

2.6 Zavvy may revoke the customer's access authorization and / or terminate the contract, if the customer considerably exceeds the use permitted to him or violates regulations for the protection against unauthorized use. In connection with this, Zavvy may interrupt or block the access to the services. Zavvy has to grant the customer in principle a reasonable grace period for remedy before. The sole revocation of the access authorization is not simultaneously considered as termination of the contract. Zavvy may maintain the revocation of the access authorization without termination only for a reasonable period of time, not exceeding 3 months.

2.7 The claim of Zavvy to a remuneration for the use exceeding the agreed use remains unaffected.
2.8 The customer shall have a claim for the re-granting of the access authorization and the access possibility after it has proven that it has ceased the use contrary to the agreement and has prevented a future use contrary to the agreement.

2.9 Zavvy shall be entitled to use the customer's logo and brand name for advertising purposes.

3. Service Levels

3.1 Zavvy shall endeavor to maintain an availability of the services of at least 99.9% per month as required for the purpose of the contract.

3.2 In case of an only insignificant reduction of the suitability of the services for the contractual use, the customer shall have no claims due to defects. The strict liability of Zavvy because of defects, which already existed at the time of the conclusion of the contract, is excluded.

3.3 Zavvy is entitled to temporarily suspend or limit the provision of the services for the performance of care and maintenance work (maintenance period). Care and maintenance work shall be performed by Zavvy during periods of low usage, if possible. This does not affect the right of Zavvy to carry out appropriate measures at any time, even without notice, in order to prevent concrete dangers to the security and integrity of the systems. These periods are not part of the guaranteed availability and service provision.

4. Modification

4.1 Zavvy may provide updated versions of the services.

4.2 Zavvy shall inform the customer about updated versions and corresponding usage instructions electronically and make them available accordingly. Updated versions may differ from the previous version in appearance and functionality. The time and scope of changes leading to a new version of the services shall be determined exclusively by Zavvy.

5. **Data Protection and Data Security**

5.1 To the extent that Zavvy has access to personal data of the customer or from the customer's domain, Zavvy shall act exclusively as a commissioned data processor and shall process and use such data only for the performance of the contract. Zavvy shall observe instructions of the customer for the handling of such data. The customer shall bear any adverse consequences of such instructions for the execution of the contract. Details for the handling of personal data shall be agreed upon by the parties in writing, as far as this is necessary according to valid legal standards.

5.2 It is agreed that the customer remains "master of the data" both generally in the contractual relationship and in the sense of data protection law. The customer is the sole owner with respect to the authority to dispose of all data used by him (entered data, processed, stored data, issued data). Zavvy and all parties involved on its side in the execution of the contract do not control the legal admissibility of the collection, processing and use of the data stored for the customer. The customer is solely responsible for the collection, processing and use of personal data.

5.3 If the customer collects, processes or uses personal data in connection with the contract, the customer warrants that it is entitled to do so in accordance with the applicable provisions, in particular the provisions of data protection law, and in the event of a violation, it shall indemnify Zavvy against claims of third parties.

5.4 Zavvy may subcontract, but shall impose on each subcontractor the corresponding obligations resulting from the contract and these terms.
Zavvy or third parties commissioned by it shall take the technical and organizational security precautions and measures to comply with the legal data protection regulations.

6. Obligations of the Customer

6.1 The customer shall protect the access authorizations as well as identification and authentication information assigned to him or to the users from access by third parties and shall not disclose them to unauthorized persons.

6.2 The customer is obligated to indemnify Zavvy against all claims of third parties due to infringements of rights, which are based on an unlawful use of the services by him or are made with his approval. If the customer recognizes or must recognize that such an infringement is imminent, the customer is obligated to inform Zavvy immediately.

6.3 The customer shall use possibilities provided by Zavvy to additionally secure its data in its original area of responsibility.
It is the customer's responsibility to properly maintain and service the software and hardware environment of the software on the mobile device, which is not covered by the contract. The customer shall protect the hardware and software in particular against unauthorized access by employees or other third parties, viruses, Trojans and other malware.

7. Customer Data

7.1 To the extent that content, materials, information and data (including personal data) originating from the customer or its users are collected, stored, executed or transmitted in the services ("**customer data**"), the customer grants Zavvy the non-exclusive, non-transferable right, limited to the contract term, to use customer data solely for the purpose of providing the services (including, without limitation, making backup copies) and related support.

7.2 If Zavvy provides new versions, updates, upgrades or extended functions of the services during the contract term, the above provisions shall also apply to such customer data.

7.3 In relation to Zavvy, the customer is the sole owner and responsible for the customer data and all results based on the customer data (e.g. videos, resulting databases, etc.). During the term of the contract, the customer and the users shall have the possibility to access, regularly retrieve and export the customer data at any time within the scope of their rights of use.

7.4 In providing the services, Zavvy shall use technical and organizational security measures in accordance with the currently recognized standards and norms in order to protect accruing or collected customer data.

8. Use in Breach of Contract**, Damages**

For each case in which the services are used without authorization in the customer's area of responsibility, the customer shall pay damages in the amount of the remuneration that would have been incurred for use in accordance with the contract within the framework of the minimum contract period applicable for this service. The use in breach of contract includes in particular customer data with pornographic content, content glorifying violence or content inciting hatred. The customer reserves the right to prove that the customer is not responsible for the unauthorized use or that there is no damage or a significantly lower damage. Zavvy remains entitled to claim further damages.

9. **Remuneration, Payment, Performance Protection, Deadlines**

9.1 Unless otherwise agreed, the price per user shall be agreed upon during the order process. The minimum number of users that will be charged is also agreed upon during the order process and can be accessed via the subscription management on Stripe.
Beyond that, the number of users can be increased dynamically by inviting additional users to the customer's Zavvy account. Every active account (user who accepted the invitation and has not been deleted) surpassing the number of users agreed upon during the order process is counted and charged as an additional user. Unless otherwise agreed, the price per user remains the same.
The overall subscription fee is calculated by multiplying the number of users by the price per user.
For additional users added or deleted during a subscription period, the subscription fee shall be charged on a pro-rata basis. This applies to both monthly and yearly contracts.
Subscription details are accessible at https://billing.stripe.com/p/login/4gw9CK3h8dKNeas288.
Remunerations are in principle net prices plus legally applicable value added tax.

9.2 For annual subscriptions, Zavvy may invoice annually in advance.

9.3 All invoices shall be paid in principle no later than 10 calendar days after receipt without deduction.

9.4 The customer may only offset or withhold payments due to defects to the extent that it is actually entitled to payment claims due to material defects or defects in title of the service. Due to other claims for defects, the customer may withhold payments only to a proportionate extent taking into account the defect. The customer has no right of retention if his claim for defects is time-barred. Apart from that, the customer may only set off or exercise a right of retention with undisputed or legally established claims.

9.5 Zavvy is entitled to prohibit the customer from further use of the services for the duration of a delay in payment by the customer. Zavvy may assert this right only for a reasonable period of time, as a rule for a maximum of 3 months. This does not constitute a withdrawal from the contract. § 449 para. 2 BGB remains unaffected.

9.6 If the customer does not settle a due claim at the contractual payment date, in whole or in part, Zavvy may revoke agreed terms of payment for all claims. Zavvy is further entitled to perform further services only against prepayment. The advance payment has to cover the respective billing period or - in case of one-time services - their remuneration.

9.7 In case of economic inability of the customer to fulfill his obligations towards Zavvy, Zavvy may terminate existing continuing obligations without notice, also in case of an insolvency application of the customer. § 321 BGB and § 112 InsO remain unaffected. The customer shall inform Zavvy early in writing about an impending insolvency.

10. Liability

10.1 The parties shall be liable to each other in full for intent, gross negligence, for claims under the Product Liability Act and in the event of injury to life, limb or health for all damages attributable thereto.

10.2 In the event of a slightly negligent breach of material contractual obligations, the parties shall be liable to each other only for the foreseeable damage typical for the contract, unless the damage claims are based on injury to life, body or health. Material contractual obligations are those whose fulfillment is necessary to achieve the objective of the contract and on whose compliance the parties may regularly rely. In such cases, liability shall be limited to the annual gross remuneration.

10.3 This clause shall also apply to the liability of a party's representatives, bodies and employees if claims are asserted directly against them.

11. Secrecy

11.1 The parties agree to maintain secrecy regarding confidential information of the respective other party. Confidential information within the meaning of this agreement shall be all business or trade secrets of a technical, commercial, organizational or other nature, in particular the terms and conditions underlying the agreement.

11.2 Excluded from the obligation to maintain confidentiality is such confidential information (i) which was demonstrably already known to the Receiving Party at the time of disclosure; (ii) which at the time of disclosure is generally known, has been published, is part of the general technical knowledge or is the general state of the art; (iii) which after the time of disclosure becomes generally known or violates the confidentiality agreement, statutory provisions or official orders; or (iv) which after the time of disclosure is independently identified or developed by the Receiving Party independently of the confidential information.

11.3 The parties shall only grant access to confidential information to such third parties (i) who are legally bound to secrecy or (ii) who require confidential information for the performance of the contract and to whom a confidentiality obligation substantially corresponding to this clause has been imposed.

11.4 The obligation to maintain confidentiality shall continue for three years after termination of the contract, but to the extent that industrial property rights are communicated as confidential information, at least until the expiration of their term of protection, whichever is longer. Insofar as a separate confidentiality agreement has been concluded between the parties, such agreement shall take precedence over the provisions of this agreement.

12. **Contract Term and Termination**

12.1 The services shall be provided by activation of the services by Zavvy for the contract term specified in the account.

12.2 During any minimum term, early ordinary termination shall be excluded by either party.

12.3 Yearly contracts may be terminated with a notice period of three months, at the earliest at the end of any minimum term. If this is not done, the contract shall be extended by a further year, unless it has been terminated with three months' notice to the end of the respective extension period.

12.4 Monthly contracts may be terminated with a notice period of two weeks, at the earliest at the end of any minimum term. If this is not done, the contract shall be extended by a further month, unless it has been terminated with two weeks notice to the end of the respective extension period.

12.5 The right of each party to extraordinary termination for good cause shall remain unaffected.

12.6 Any notice of termination must be in writing to be effective. Text form shall also suffice.

12.7 Upon termination of the agreement, Zavvy shall be entitled to block the customer's access to the services and to delete all customer data and other data of the customer, unless applicable laws mandatorily require further retention of such data. The retained data shall be subject to the confidentiality obligation pursuant to Section 11.

13. Final Provisions

13.1 This agreement (including any attachments) fully reflects the understanding of the parties with respect to its subject matter. There are no ancillary agreements.

13.2 If any provision of this agreement or part thereof is or becomes invalid or unenforceable, this shall not affect the validity and enforceability of the remainder of the agreement. The parties undertake to replace the invalid or unenforceable provision or the invalid or unenforceable part of a provision by a valid and enforceable provision which comes as close as possible to the economic purpose and which the parties would have agreed if they had known of the invalidity or unenforceability at the time of concluding this agreement. The foregoing shall apply mutatis mutandis to gaps in this contract. § Section 139 of the German Civil Code (BGB) shall not apply, not even as a rule of burden of proof.

13.3 This agreement shall be governed by German law.

13.4 The exclusive place of jurisdiction for all disputes arising from or in connection with this contract or concerning its validity shall be Munich, Germany, to the extent legally permissible.

Agreement

on the Processing of Personal Data within the scope of Article 28(3) of Regulation (EU) 2016/679 (GDPR)

– Data Processing Agreement –

On behalf of **the customer** (as defined in the Terms of Service)
– Controller within the scope of Article 4(7) of the GDPR –
– hereinafter referred to as the “Controller” –

by Zavvy Gmbh
Rosental 7 80331 Munich
Germany

– Processor within the scope of Article 4(8) of the GDPR –
– hereinafter referred to as the “Processor” –

– hereinafter jointly referred to as the "Parties" –

§ 1 | Subject Matter and Duration of the Processing

(1) Subject matter

The agreement placed by the Controller with the Processor shall include the following activities and/or services: Provision, support, maintenance and (remote) servicing of an online learning platform

(2) Duration

[1]This agreement is executed with the signature of both Parties and runs for an indefinite period of time. [2]Each Party has the right to terminate this agreement with due notice of four weeks to the end of the month pursuant with the written form and meaning of § 126 BGB (German Civil Code). [3]In the absence of a termination date, the Controller may terminate this agreement at any time and without prior notice if the Processor has committed a serious breach of the data

protection regulations or the provisions of this agreement, if the Processor is unable or unwilling to carry out the instructions from the Controller or, if the Processor refuses the Controller´s control rights. [4]The Parties acknowledge that no (further) data processing may be carried out without the existence of a valid processing agreement.

§ 2 | Specification of the Data Processing

(1) Type of Processing

[1]Within the scope of this agreement, personal data shall be processed by the Processor pursuant to Article 4 no. 2 GDPR. [2]In particular, this involves the collection, recording, organization, arrangement, storage, adaptation or modification, reading out, querying, use, disclosure by transmission, matching or linking.

(2) Purpose of Data Processing

The data is processed for the following purpose:

- Setting up role cards and career paths
- Conducting feedback
- Assigning and recommending courses
- Tracking of user progress
- Insight into learning focus
- User experience improvements
- Undertaking of surveys

(3) Place of Processing

[1]The performance of the contractually agreed data processing takes place in principle in a Member State of the European Union (EU) or in another Contracting State to the Agreement on the European Economic Area (EEA). [2]The Processor is nonetheless permitted to process personal data outside the EEA in compliance with the provisions of this agreement, provided that, he informs the Controller in advance of the location of the data processing and if the requirements of Art. 44 et seq. GDPR are met.

(4) Type of Data

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

- Personal Master Data (Key Personal Data)
- Product Data as used by the Controller

(5) Categories of Data Subjects
The categories of data subjects affected by the processing include:

- Employees

§ 3 | Technical and Organizational Measures

(1) [1]The Processor shall document the implementation of the Technical and Organizational Measures set out, prior to the award of this agreement and the commencement of the processing, in particular regarding the specific execution of this agreement and deliver thereafter, the corresponding documentation to the Controller for review. [2]If accepted by the Controller, the documented measures become the basis of this agreement. [3]If the inspection or an audit of the Processor proves a need for adjustment, such adjustments shall be implemented pursuant to this agreement.
(2) [1]The Processor shall establish the security pursuant to Art. 28 para. 3 (lit. c and lit. e) and Art. 32 GDPR, in particular, in conjunction with Art. 5 paras. 1 and 2 GDPR. [2]The actions to be adopted are data security measures and measures that guarantee a protection level appropriate to the risk concerning confidentiality, integrity, availability and resilience of the systems and services. [3]In doing so, the state of the art, the implementation costs and the nature, scope and purpose of the processing, as well as the different probability and severity of the risk for the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be considered (details in Annex 1).
(3) [1]The Technical and Organizational Measures are subject to technical progress and further development. [2]In this respect, the Processor may implement adequate and alternative measures. [3]In doing so, the security level of the specified measures must not be reduced. [4]Significant changes shall be documented.

§ 4 | Quality Assurance and other Obligations of the Processor pursuant to Article 28 para. 3 sentence 1 GDPR

In addition to complying with the provisions of this agreement, the Processor has its own statutory obligations as a processor; in particular, he ensures compliance with the following specifications:
a) [1]To the extent required by law, the Processor appoints a competent and reliable person as a data protection officer, who shall perform his duties pursuant to Art. 38 and 39 GDPR. [2]The contact details of the designated data protection officer will be communicated to the Controller for the purpose of allowing a direct contact. [3]If the Processor is not obliged to designate a data

protection officer, he shall designate a contact person for data protection matters whose data shall be communicated to the Controllers for the purpose of allowing a direct contact. [4]All changes to the designated data protection officer or the contact person must be reported to the Controller without delay. [5]If the Processor is not established in the European Union, he shall designate a representative in the European Union pursuant to Art. 27 GDPR. [6]The contact information of the representative as well as any changes to the designated representative shall be immediately notified to the Controller.

b) Pursuant to Art. 28 para. 3 sentence 2 lit. b GDPR, the Processor guarantees that the persons authorized to process personal data have agreed to maintain confidentiality or are subject to an appropriate statutory secrecy duty and have been previously familiarized with the relevant data protection provisions.

c) The Processor and any person subordinate to the Processor who has access to personal data may only process personal data according to the instructions of the Controller (Art. 29, 32 para. 4 GDPR), including the powers granted in this agreement with the exception that they are legally bound to do so.

d) The Processor guarantees the implementation and compliance with all Technical and Organizational Measures required under this agreement pursuant to Art. 28 para. 3 sentence 2 lit. c, Art. 32 GDPR (details in Annex 1).

e) Upon request, the Controller and the Processor (and if applicable, their representative) shall cooperate with the supervisory authority in the performance of their tasks (Art. 31 GDPR).

f) [1]The Processor shall inform the Controller without undue delay of any supervisory acts and measures concerning the processing insofar as they relate to this Agreement. [2]The foregoing is also applicable if a competent authority investigates the processing of personal data by the Processor in the context of an administrative offense or criminal proceedings.

g) Provided that the Controller is subject to inspection by the supervisory authority, an administrative or criminal procedure, the liability claim of a data subject or a third party or any other claim in connection to the processing by the Processor, the Processor shall use his best efforts and support the Controller to the best of its ability.

h) The Processor shall regularly review his internal processes and Technical and Organizational Measures to ensure that the processing within his area of responsibility complies with the requirements of the applicable data protection law and that the protection of the data subject's rights is ensured.

i) The Processor guarantees the verifiability of the Technical and Organizational Measures adopted towards the Controller within the scope of his control powers pursuant to § 6 of this agreement.

§ 5 | Conditions for Subcontracting pursuant to Art. 28 para. 3 sentence 2 lit d GDPR in conjunction with Art. 28 paras. 2 and 4 GDPR

(1) [1]Subcontracting means services directly related to the performance of the main service. [2]Notwithstanding the aforementioned, the services that the Processor contracts with third parties as a mere ancillary service in order to carry out business activities are not to be regarded as subcontracting. [3]These include, for example, cleaning services, pure telecommunication services without specific reference to services provided by the Processor for the Controller, postal and courier services, and transport or security services. [4]Despite the above, the Processor shall ensure, even with ancillary services provided by third parties, that appropriate precautions and Technical and Organizational Measures have been adopted to ensure the protection of personal data. Also, the maintenance and servicing of IT systems or applications constitute a subcontracting agreement subject to approval and data processing within the meaning of Art. 28 GDPR, provided that the maintenance and testing concern the systems used in connection with the performance of services for the Controller and, if the personal data processed on behalf of the Controller may be accessed during said maintenance.

(2) Pursuant to Art. 28 para. 2 sentence 1 GDPR, the Processor may not use any additional processors (subcontracted or sub-subcontracted) without the prior separate or general written authorization of the Controller whereby all subcontracting provisions shall apply for both the subcontractor and to any subsequent used (sub-) subcontractor.

(3) The Controller hereby agrees to the following subcontractors:

Name/Company	Address/Country	(Partial) Service	Data location
Sendinblue	Sendinblue 7 rue de Madrid 75008 Paris, France	Email management	EU (France, Belgium, Ireland)
AWS	Amazon Web Services Inc. 410 Terry Avenue North Seattle, WA 98109-5210, USA	Cloud infrastructure	Germany
Datadog	Datadog, Inc. HQ: 620 8th Ave 45th Floor New York, NY 10018 USA Germany: Rothofstraße 13-19	Application monitoring	Germany

	60313 Frankfurt, Germany		
Sentry	Functional Software Inc. HQ: 45 Fremont Street, 8th Floor San Francisco, CA 94105, USA Europe: Rothschildplatz 3/2/ab, 1020 Wien, Austria	Error tracking	Self-hosted (Germany)
Matomo	InnoCraft Ltd 7 Waterloo Quay Wellington, Wellington 6011, NZ	Web analytics	Germany
Crisp	Crisp IM SARL 2 Boulevard de Launay 44100 Nantes, France	In-App Chat	EU (NL,DE,IE)
Optional services			
Nylas	Nylas, Inc. 944 Market Street, 8th Floor San Francisco CA 94102, USA	Calendar Integration	EU (Ireland)
Mailchimp	The Rocket Science Group, LLV, 675 Ponce de Leon Ave NE, Suite 5000, Atlanta, GA 30308 USA	Email management	USA
WorkOS	WorkOS, Inc. 548 Market Street #86125 San Francisco CA 94104, USA	HRM integrations & Single Sign On	USA
Stripe	Stripe Payments Europe, Limited The One Building, Grand Canal Street Lower, Dublin 2, Ireland	Payment Services Provider	EU (Irleand) / USA
Kombo	Kombo Technologies GmbH c/o Factory Works GmbH	HR Integrations (non native)	EU

	Lohmühlenstraße 65 12435 Berlin		
OpenAI	OpenAI OpCo LLC 3180 18th St. San Francisco CA 94110 USA	AI functionalities	USA

(4) [1]The transfer of personal data of the Controller to the subcontractor and its initial action shall only be permitted upon presentation of all conditions for subcontracting. [2]In particular, it is the Processor's responsibility to transfer his data protection obligations set under this agreement to additional processors pursuant to Art. 28 para. 4 sentence 1 GDPR.

(5) [1]If the subcontractor provides the agreed service outside the EU/EEA, the Processor shall ensure that compliance with data protection law is fulfilled through appropriate measures. [2]The same will apply if service providers within the meaning of para. 1 sentence 2 are to be used.

(6) Further outsourcing by the subcontractor is permitted. All contractual provisions in the chain of contract shall also be imposed on the further subcontractor.

§ 6 | Control Rights of the Controller pursuant to Art. 28 para. 3 sentence 2 lit. h GDPR

(1) [1]The Controller has the right to carry out inspections in consultation with the Processor or to appoint auditors who are not allowed to compete with the Processor to carry out the inspections in individual cases. [2]The Controller has the right to verify the compliance of the Processor with this agreement in his business operations by means of random checks, which are usually, timely announced in advance.

(2) [1]The Processor shall ensure that the Controller can verify compliance with the obligations of the Processor under Art. 28 GDPR. [2]The Processor undertakes to provide the Controller with the necessary information upon request and, in particular, to evidence the implementation of the Technical and Organizational Measures.

(3) Evidence of such measures, which do not only concern the concrete processing, may be provided by:

a. compliance with the approved codes of conduct pursuant to Art. 40 GDPR;

b. certification according to the approved certification procedure established in Art.42 GDPR;

c. current certificates, reports or report extracts of independent bodies (e.g. auditors, inspectors, data protection officers, IT security departments, data protection auditors, quality auditors); and/or

d. appropriate certification through an IT security or data protection audit (e.g. according to the Federal Office for Security in Information Technology, BSI Grundschutz).

§ 7 | Support and Notification Obligations of the Processor pursuant to Art. 28 para. 3 sentence 2 lit. e and f GDPR

(1) [1]The Controller is responsible for safeguarding the rights of data subjects. [2]In this context, the Processor is nonetheless obligated, depending on the type of processing, to support the Controller – to the extent possible – with suitable Technical and Organizational Measures to fulfill the Controller's obligations in regard to the rights of the data subjects referred to in Chapter III of the GDPR, that is to say, when responding to data subjects´ inquiries concerning the Controller's information obligations to the data subjects, their right of access, their right of rectification, erasure, restriction of processing, data transferability and related communication obligations of the Controller, the right to object to automated decisions, including profiling if the data subject asserts any such rights. [3]If the data subject complains at the Processor with the purpose of asserting a right, the latter forwards the inquires to the Controller without delay.

(1) [1]Considering the nature of the processing of the agreement and the information available to the Processor, the Processor must assist the Controller in compliance with the obligations set out in Articles 32 to 36 of the GDPR, i.e. in the performance the Controller's legal obligations on data security, reporting data breaches to the supervisory authorities and the data subjects, implementing data protection impact assessments and in consulting the competent supervisory authority beforehand, provided that this is required by the data protection impact assessment. [2]The Processor and the Controller shall cooperate in response to inquiries from the relevant supervisory authorities in the performance of their duties.

§ 8 | Authority of the Controller

(1) [1]The Processor shall process personal data exclusively within the framework of the agreements in place and pursuant to the instructions of the Controller, unless otherwise required under the laws of the European Union or of the Member State to which the Processor is subject (Art. 28 para. 3 sentence 3 lit. a, Art. 29 GDPR). [2]In the event of such obligation, the

Processor shall notify the Controller of these legal requirements prior to the processing unless such notification is prohibited by the law on ground of a prevailing public interest.

(2) [1]The Processor warrants that the processing will be carried out pursuant to the instructions of the Controller. [2]If the Processor is of the opinion that an instruction of the Controller violates this agreement or the applicable data protection law, he shall immediately inform the Controller. Following a corresponding notification to the Controller, the Processor is entitled to suspend the execution of the instruction until confirmation or amendment of the instruction by the Controller. [3]The Parties agree that the sole responsibility for the instructed processing lies with the Controller.

(3) [1]The Controller's instructions are always in written or text form. [2]If necessary, the Controller may also give verbal instructions (remotely). [3]Verbally issued remote instructions shall be confirmed immediately by the Controller in written or text form.

§ 9 | Erasure and Return of Personal Data pursuant to Art. 28 para. 3 sentence 2 lit. g GDPR

(1) [1]Copies or duplicates of the data shall not be made without the knowledge of the Controller. 2This excludes backup copies, to the extent necessary to ensure proper data processing, as well as data copies required with regard to statutory retention requirements.

(2) [1]Upon completion of the contractually agreed work, or sooner, upon request by the Controller – at the latest, upon the termination of the Main Agreement – the Processor shall deliver all documents related to the contractual relationship to the Controller, or destroy them after prior consent in accordance with data protection regulations after receiving prior consent from the Controller. [2]The same applies to test and reject materials. 3Instructions for deletion shall be submitted upon request.

(3) [1]Documentation serving as proof of orderly and proper data processing shall be kept by the Processor according to the respective retention periods beyond the end of this agreement. [2]The Processor may hand the documentation over to the Controller at the end of the agreement for his release.

§ 10 | Miscellaneous

(1) [1]Both Parties shall treat with confidentiality all knowledge of trade secrets and data security measures of the other Party acquired within the scope of the contractual relationship and even after the end of this agreement. [2]If there is any doubt as to whether information is subject to confidentiality, it shall be treated as confidential pending written approval of the other Party.

(1) If the Processor's property is endangered by measures taken by third parties (such as seizure or confiscation), insolvency or settlement proceedings or other events, the Processor shall notify the Controller immediately.

(3) [1]For additional agreements, the written form is required. [2]Waiver of this requirement must also be in writing.

(4) The defense of the right of retention, irrespective of the legal grounds, shall be excluded with regard to the data processed in the context of this Agreement and with regard to relevant data carriers.

(5) This agreement shall also apply if and to the extent that authorities or courts deviate mutatis mutandis from a joint responsibility of the contracting parties pursuant to Art. 26 GDPR.

(6) [1]Should individual provisions of this agreement prove to be wholly or partially invalid or unenforceable or become invalid or unenforceable as a result of changes in applicable legislation after the conclusion of this agreement, its remaining provisions and the validity of this agreement as a whole shall remain unaffected. [2]The invalid or unenforceable provision shall be replaced by an effective and enforceable provision that comes as close as possible to the purpose of the invalid provision. [3]If the agreement should prove to be incomplete, such provisions shall be deemed to have been agreed upon as if there was adequate consideration.

(7) This agreement is exclusively subject to the laws of the Federal Republic of Germany with the exception of the referenced international laws.

(8) The exclusive place of jurisdiction for all disputes arising out of or in connection with this agreement is the domicile of the Controller/Processor.

Annex 1:

Questionnaire for Data Processing

TECHNICAL AND ORGANIZATIONAL MEASURES

Zavvy GmbH
Updated: 07.07.2022

Physical Access Control
☒ Servers are located in an external facility
☒ No servers are being maintained within the office premises
☒ Physical protection of the company premises (lockable doors)
☒ Additional protection of the premises (alarm system, gatekeeper, security guard)
☒ Access control system on company premises (chip cards, locks)
☒ Access organization (logging and escorting visitors)
☒ Access authorization structure limited to the most necessary (incl. server access)
☒ Access control for rooms with personal data
☒ Administration and logging for keycards and physical keys
☒ Employees are obligated to store any personal data in a secure location upon leaving their workplace (clean desk policy)

Date Medium Control
☒ Locked / Secure storage
☒ Logging of inventory for data carriers like laptops and phones
☒ Electronic data carriers are being encrypted
☒ Lockable containers at every desks
☒ Employee obligation to secure storage of devices

Digital Access Control
☒ Password complexity (at least 3 of the 4 criteria: Upper case letter, lower case letter, special character and number)
☒ Password with minimum length of 8 characters
☒ No time-based change of passwords
☒ Group-wide auto logout after defined time (10 minutes)
☒ Authentication of users (user name & password)
☒ Use of a password manager with secure encryption
☒ Password policy or system-side requirement of password requirements.
☒ Personal data can be deleted on demand

User Control
☒ Obligation to maintain confidentiality or to be subject to a duty of confidentiality
☒ Dedicated administrators for every IT system
☒ IT administrators are selected for their qualification
☒ Need-to-know or Principle of Least Privilege implemented (authorization structure limited to the most necessary)
☒ Regular staff training on topics like data privacy, updates, obligation to data secrecy, password guidelines
☒ Remote workers are taught to follow guidelines for secure remote work
☒ Role-based authorization management and regular recertification of authorizations

Transmission Control
☒ Encryption for critical data during data transmission
☒ No physical data carriers are used to transfer personal data

Recoverability
☒ Data protection concept (backup concept) incl. regular backups
☒ Secure storage of data backups
☒ Recoverable data include logs, user accounts, configurations including settings and permissions
☒ The organization has created an an emergency admin access in printed form

Reliability
☒ Updates and/or patch and vulnerability management

Order Control
☒ Selection of contractors under due diligence aspects
☒ A DPA has been signed with all subcontractors
☒ The organization has established criteria for selecting suppliers
☒ The organization has defined written criteria for selecting suppliers

Data Integrity
☒ Virus protection and anti-malware
☒ Regular updates of technical and organizational measures
☒ A security assurance plan has been defined in writing
☒ There is a defined incident response plan for any possible vulnerability with different layers

of urgency

Separability
☒ Separation into test, production and development levels
☒ Separation of data processing (logical or physical), multi-client capability