



General terms and conditions about software of the MATE Development GmbH ("GTC")

Status: 19.12.2023

These terms and conditions have been translated automatically. Please check the German version under <https://to.sweap.io/agb> for a legally secure version.

MATE Development GmbH, Rankestraße 9, 10789 Berlin, registered with the Charlottenburg Local Court under HRB 174234 B, represented by the managing directors Florian Kühne, Matthias Heicke and Sven Frauen (hereinafter referred to as "**Sweap**") offers software products under the Sweap brand to entrepreneurs in the exercise of their business or independent professional activities within the meaning of § 14 BGB (German Civil Code) ("**Customers**") via the website sweap.io.

The customers wish to use these products for the purpose of better event and organization management within their respective companies as a web-based SaaS or cloud solution according to the product description limited to the period of the existence of this contract.

Any general terms and conditions of the customer do not apply to Sweap, regardless of whether Sweap has expressly objected to their application or not.

1. Subject matter of the contract

- (1) The terms and conditions of these GTC apply to the use of the software 'Sweap' in accordance with the respective current product description at <https://sweap.io> ("**Product Description**") (depending on the current product description, the "**Software**").
- (2) The software is operated by Sweap as a web-based SaaS or cloud solution. The customer is thereby enabled to use the software stored and running on the servers of Sweap or a service provider commissioned by Sweap for its own purposes via a connection to the Internet during the term of the contract in accordance with these GTC and to store, process or use its data or content uploaded by it and to integrate elements of the software, such as certain login pages and forms, into its own websites.

2. conclusion of contract

- (1) The customer can register via the website sweap.io, indicating the name, company, e-mail address and VAT number, and thus makes an offer to conclude these GTC, whereupon Sweap checks the registration.

and sends a confirmation e-mail to the customer and in the following with the receipt of the confirmation e-mail by the customer the contract is deemed to be concluded ("**start date**").

- (2) The customer is then provided by Sweap with the access data to an account, which can be called up on the website sweap.io, into which the customer can then log in in order to use the services of Sweap ("**account**").

3. services of Sweap

- (1) Sweap provides the customer with the software in its most current version for use at the router exit of the data center in which the server with the software is located ("**handover time**"). The software, the computing power required for use and the required storage and data processing space are provided by Sweap. However, Sweap does not owe the establishment and maintenance of the data connection between the customer's IT systems and the described handover point.
- (2) Insofar as the software runs exclusively on the servers of Sweap or another commissioned service provider, the customer does not require any copyright usage rights to the software and Sweap does not grant any such rights.
- (3) For the term of the respective license to be remunerated, Sweap grants the customer the non-exclusive, non-transferable right, limited in time to the term of the contract in accordance with these GTC, to load the user interface of the software for display on the screen into the main memory of the end devices used for this purpose in accordance with the contract and to make the resulting copies of the user interface. The Customer hereby accepts the granting of these rights.
- (4) The support services in the sense of these GTC (see clause 8) include the delimitation of the cause of the error, the error diagnosis as well as services aimed at the elimination of the error (in particular patches and service packs). Sweap assumes no responsibility for the elimination of the error.

4. availability of the software

- (1) Sweap draws the customer's attention to the fact that restrictions and/or impairments to the services provided may arise that are beyond Sweap's control, such as actions by third parties not acting on behalf of Sweap, technical conditions beyond Sweap's control, and force majeure.
- (2) The hardware, software and technical infrastructure used by the customer may also have an influence on the services provided by Sweap. Insofar as such circumstances have an influence on the availability and/or functionality of the services provided by Sweap, this has no effect on the contractual conformity of the services provided.
- (3) The customer is obligated to immediately report functional failures, malfunctions or impairments of the software to Sweap via the integrated reporting function within the software and to name these as precisely as possible or, if the reporting function within the software is affected by the malfunction, the customer must notify Sweap of the corresponding case of malfunction by e-mail to support@sweap.io. If the customer fails to do so, the provision of § 536c BGB shall apply accordingly.

5. data processing rights; data backup

- (1) Sweap acts in accordance with the applicable legal provisions on data protection. The current data protection provisions of Sweap apply, available at <https://sweap.io/privacy-policy>.

- (2) For the purpose of executing the contract according to these GTC, the customer grants Sweap the right to duplicate the data to be stored by Sweap for the customer, as far as this is necessary to provide the services owed according to these GTC. Sweap is also entitled to keep the data in a failover system or separate failover computer center. In order to eliminate malfunctions, Sweap is also entitled to make changes to the structure of the data or the data format.
Sweap hereby accepts the granting of these rights.
- (3) Sweap regularly backs up the customer's data on the server for which Sweap is responsible on a backup server. The customer can, as far as technically possible, excerpt this data at any time for backup purposes and is obliged to do so at regular intervals.

6. data processing

- (1) If and insofar as the customer processes or uses personal data on IT systems for which Sweap is responsible, the parties shall conclude a data processing agreement.
- (2) Sweap uses the client data exclusively in accordance with the client's instructions as they are conclusively expressed in the provisions of the data processing agreement. Individual instructions that deviate from the stipulations of the data processing agreement or impose additional requirements require the prior consent of Sweap and take place after contact of the customer by e-mail at least in text form according to § 126b BGB. Any additional costs arising from these individual instructions are to be borne by the customer and are to be paid to Sweap after prior invoicing by Sweap in accordance with clause 9 of these GTC below.
- (3) Sweap and the Customer undertake to conclude an adapted version of such data processing agreement in each case, should this become necessary, for example for reasons of changes in the law.

7. contents of the customer

- (1) The customer has the possibility to upload content (such as data, graphics, images, texts, diagrams, files, etc.) within his account ("**customer content**").
- (2) The customer is solely responsible for this customer content and undertakes not to upload or otherwise use any prohibited content pursuant to section 13 (1) of these GTC within his account.
- (3) As a matter of principle, Sweap does not claim ownership of these customer contents.
- (4) Insofar as the customer provides Sweap with these customer contents, the customer grants Sweap all rights necessary for the execution of the contractual agreement (e.g. in case of a change of the domain of Sweap). This includes in particular the right to make the corresponding content available to the public. Sweap hereby accepts this granting of rights.
- (5) In the event that customer content is removed from an account or that an account is/will be deleted by the customer or by Sweap - for whatever reason - the rights of Sweap to the respective customer content expire.

8. service and support services

- (1) A "**service case**" exists if the software does not fulfill the contractual functions according to the product description, delivers incorrect results, data processing breaks down in an uncontrolled manner or does not function properly in any other way, so that the use of the software is not possible or only possible to a limited extent.

- (2) The customer can report a service case to Sweap via the integrated reporting function within the software. If for any reason the reporting function within the software is not functional, then the customer can report the service case by e-mail to support@sweap.io, whereby Sweap will be available during the service hours on weekdays (Berlin), Monday to Friday between 9 a.m. and 6 p.m. ("**service hours**"). In doing so, the customer is obligated to provide as detailed a description as possible of the respective functional failure, malfunction or impairment at least in text form in accordance with § 126b BGB (e.g. by e-mail).

9. remuneration

- (1) Insofar as Sweap offers a demo or other limited version, this is free of charge in accordance with the terms and conditions described on the website sweap.io.
- (2) Furthermore, the customer pays for the services owed by Sweap according to these GTC or the granting of rights a remuneration plus the statutory value added tax. The amount as well as further regulations regarding the remuneration result from the price table attached to the product description at <https://sweap.io/pricing>.
- (3) Payment of the remuneration shall be made through a payment method provided on Sweap's website at <https://sweap.io/pricing>.
- (4) Unless otherwise agreed between the parties, the remuneration is due for payment within fourteen 14 calendar days from the date of receipt by the customer of a corresponding invoice from Sweap.
- (5) If the customer defaults on a payment or if a return debit note is issued, Sweap reserves the right to claim damages for default (e.g. collection fees, reminder fees, default interest and chargeback fees).

10. obligations of the customer

- (1) The customer shall support Sweap in the provision of the contractual services to a reasonable extent.
- (2) The customer is responsible for the proper and regular backup of his data. The same applies to Sweap with regard to the documents provided during the execution of the contract.
- (3) For the use of the software according to these GTC, the system requirements resulting from the product description must be fulfilled by the customer. The customer is responsible for this himself.
- (4) The customer is aware that Sweap does not operate its own network and does not provide the customer with Internet access. For this reason, Sweap assumes no responsibility for the functionality of the respective access to the Internet.
- (5) All requested data or customer content must be provided completely and correctly, provided that the request for such data does not violate any (data protection) law(s).
- (6) As far as the customer provides Sweap with customer content, he assures to own all necessary rights to the provided customer content in order to grant Sweap the corresponding rights.
- (7) The Account (including the Admin Profile as well as sub-profiles created by the Admin for employees of the Customer) must be secured with a password, and the Customer must immediately change the password originally provided to a secure password. Customer

shall take all necessary steps to ensure the confidentiality of the password and shall ensure that any employees to whom the access data is provided do likewise. Each customer is obligated to immediately notify Sweap at support@sweap.io if there are indications that his account has been compromised by third parties who are not employees of the customer or of a company affiliated with the customer pursuant to §§ 15 et seq. AktG (German Stock Corporation Act) ("**third parties**").

- (8) The customer is not entitled to grant third parties access to an account opened in his name or to make the service of Sweap available to third parties, unless the parties have expressly agreed otherwise in compliance with the statutory written form.
- (9) In the context of sending e-mails with our e-mail service provider Mailjet, Sweap is obligated to comply with the "Acceptable Use Policy of Mailjet" (<https://www.mailjet.com/sending-policy/>). The Customer is likewise obliged to comply with these guidelines towards Sweap. If these guidelines are not followed by the Customer, the use of emailing may be restricted. In some cases, this may lead to a temporary or permanent blocking of email sending.

11. warranty

- (1) In principle, the statutory provisions on warranty in rental agreements apply. The regulations in § 536b BGB (knowledge of the tenant of the defect upon conclusion of the contract or acceptance) and in § 536c BGB (defects occurring during the rental period; notification of defects by the tenant) apply. However, the application of Section 536a (2) of the German Civil Code (tenant's right of self-remedy) is excluded. The application of Section 536a (1) BGB (Landlord's liability for damages) is also excluded insofar as the standard provides for strict liability.
- (2) In all other respects, the provisions of the law on service contracts (§§ 611 et seq. BGB) shall apply.

12. liability

- (1) Any liability of Sweap for damages caused by or in connection with the performance of duties under this contract is excluded. A limitation of liability does not apply to
 - Damages resulting from injury to life, body or health;
 - Damages that are based on a breach of duty by Sweap with regard to essential contractual rights and obligations that are indispensable for the proper execution of the contract, and through this the achievement of the purpose of the contract is endangered (cardinal obligations), whereby liability in this case is limited to typical and foreseeable damages;
 - Damages that are based on an intentional or grossly negligent breach of duty by Sweap;
 - liability under the Product Liability Act;
 - liability in the event of the assumption of a guarantee;
 - claims bases under data protection law.
- (2) The exclusion of liability and the limitations of liability of Sweap also apply to the legal representatives and vicarious agents of Sweap.
- (3) Sweap is not liable for damages due to labor disputes and/or force majeure.

13. customer data and exemption

- (1) As a technical service provider, Sweap stores content and data for the customer, which the customer enters and stores when using the software and makes available for retrieval.

The customer undertakes vis-à-vis Sweap not to post any content and data that is punishable by law or otherwise illegal in absolute terms or in relation to individual third parties and not to use any viruses or other programs containing malware/malicious software in connection with the software. In particular, he undertakes not to use the software to offer illegal services or goods. The customer is the responsible party with regard to personal data of himself and his users/employees and must therefore always check whether the processing of such data via the use of the software is supported by the relevant permissions or, if necessary, obtain the relevant consents of the persons concerned.

- (2) The customer is solely responsible for all content and processed data used by him or his users as well as the legal positions required for this. Sweap does not take any notice of contents of the customer or his users/employees and basically does not check the contents used with the software.
- (3) Sweap will receive data from the customer in the course of providing the services according to these GTC, as shown in section 5. This may include email addresses, among other things. In principle, Sweap is not in a position to check whether, in accordance with the planned use of the data in accordance with these GTC by Sweap itself or on behalf of the customer, the legal requirements, such as an express consent of the person concerned or compliance with the consent procedure regarding the sending of advertising (such as double-opt-in) have been met and there is no revocation of consent or consent. This is the sole responsibility of the customer.
- (4) The customer and Sweap clarify that no special personal data, i.e. information about racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life, are processed in the context of the provision of services by Sweap or use of the software. The customer agrees to comply with this requirement and to inform Sweap immediately in case of misuse.
- (5) In this context, the customer undertakes to indemnify Sweap or representatives, employees and vicarious agents of Sweap against any liability and costs (including possible and actual losses, damages, expenses, costs, lawsuits, claims, court proceedings, legal disputes, actions, obligations, claims and liability claims), if a claim is made against Sweap by third parties or employees of the customer personally, as a result of alleged acts or omissions of the customer and the customer is responsible for the infringement. Sweap will inform the customer about the claim and, as far as this is legally possible, give the customer the opportunity to defend the asserted claim. At the same time, the customer will provide Sweap with all available information that is necessary for a review of the asserted claims and for their defense. The customer shall provide this information promptly, truthfully and completely. Customer agrees not to settle any claim without the prior written consent of Sweap.
- (6) Any further claims for damages by Sweap remain unaffected.

14. contract term and termination; validity of acquired licenses; export option

- (1) The term of this contract begins on the Start Date.
- (2) Acquired single licenses regarding the software are valid until the creation of an event within the Sweap software, but no longer than 12 months from the start date. After the creation of an event, after the expiration of the 12 months from the start date or when a cancellation of the associated account becomes effective, the respective acquired licenses lose their validity without requiring a separate cancellation.

- (3) Runtime licenses are purchased for the minimum duration of 12 months from the start date. The contract is automatically renewed for another 12 months, unless it is terminated by one of the contracting parties with a notice period of (1) month to the end of the contract.
- (4) Acquired runtime licenses for agencies are closed for the duration of 1 to 12 months from the start date depending on the license variant selected.
 - The Sweap Agency license (M) is purchased from the start date for the minimum duration of (1) month. The contract is automatically extended by (1) further month, unless it is terminated by one of the contracting parties with a notice period of (2) weeks to the end of the month.
 - The Sweap Agency License (Y) is purchased for the minimum duration of (12) months from the Start Date. The contract is automatically renewed for (12) further months, unless it is terminated by one of the contracting parties with a notice period of (1) month to the end of the contract.

For purchased single licenses within the scope of a runtime license for agencies, the regulations from §14 (2) of this contract apply.

- (5) Both for this contract and for purchased licenses for the software, the right of each party to extraordinary termination for good cause remains unaffected. An important reason for the termination of this contract exists for Sweap in particular if
 - the Customer fails to meet its obligation to pay remuneration in accordance with Section 9 of this Agreement within two (2) consecutive dates despite a reminder and the setting of a deadline;
 - insolvency proceedings have been opened against the assets of a contractual partner or the opening of such proceedings has been rejected for lack of assets.
- (6) The termination must be in text form (email is sufficient) in order to be effective.
- (7) After termination of the contract, Sweap shall return to the customer all documents provided by the customer and still in Sweap's possession as well as data carriers that are related to the contract in accordance with these GTC and delete the data stored at Sweap, provided that no retention periods or rights exist. However, in the event of proper termination, the customer shall be granted the right to export the data and information stored within the contractual software within 30 days of the effective date of termination, whereby the customer may make a copy of the data and information stored on an external data storage device, which the customer may then use solely for internal purposes.

15. confidentiality

- (1) The parties are obligated to keep permanently secret, not to disclose to third parties, record or otherwise exploit all information about the respective other party that has become known to them or becomes known to them in connection with this Agreement and that is marked as confidential or is identifiable as business and trade secrets on the basis of other circumstances ("Confidential Information"), unless the respective other party has expressly consented to the disclosure or exploitation in compliance with the statutory written form or the information must be disclosed by law, court decision or an administrative decision.
- (2) The information is not confidential information within the meaning of the provisions of this Section 15 if it is

- were already previously known to the other party without the information having been subject to a confidentiality obligation;
- are generally known or become known without breach of the assumed confidentiality obligation;
- disclosed to the other party by a third party without breach of a confidentiality obligation.

(3) The obligations of the provisions of this Clause 15 shall survive the termination of the Agreement in accordance with these GTC.

16. assignment and transfer to third parties

The customer cannot transfer the rights and obligations from the contract according to these GTC to third parties without the prior written consent of Sweap. Sweap is entitled to entrust third parties with the fulfillment of the obligations arising from this contract.

17. completeness and contract amendments

- (1) This Agreement, together with the Annexes, each of which shall be deemed an integral part of this Agreement, constitutes the entire understanding between the Parties.
- (2) Amendments and supplements to this agreement must be made in writing to be effective. This also applies to the waiver of the written form requirement. Terms and conditions of the customer or third parties shall only become part of the contract if and insofar as Sweap has expressly agreed to their validity in writing.

18. miscellaneous

- (1) The present contract shall be governed by German law to the exclusion of the UN Convention on Contracts for the International Sale of Goods.
- (2) In the event that the customer, like Sweap, is a merchant within the meaning of §§ 1 ff. HGB (German Commercial Code), the contracting parties agree that Sweap's registered office shall be the exclusive place of jurisdiction for all disputes arising from and in connection with this contract.
- (3) In the event of the invalidity of one or more provisions of this contract, the parties shall agree on a replacement provision that comes as close as possible to the invalid provision.
- (4) The invalidity of one or more provisions of this contract shall not affect the validity of the remaining provisions.
- (5) In the event of contradictions between these GTC and provisions from the annexes to these GTC, the provisions from the annexes shall take precedence over those from these GTC.

List of facilities:

Appendix 1: Data processing agreement

Appendix 1: Data processing agreement (DPA)

Data processing agreement on behalf according to Art. 28
DSGVO and § 62 BDSG

between

Customer according "GTC"

("Principal") and

MATE Development GmbH, Rankestraße 9, 10789 Berlin
("Contractor")

Preamble

The Client has commissioned the Contractor with the implementation of a digital guest management in accordance with the "General Terms and Conditions on Software of MATE Development GmbH" ("GTC"). Reference is made to the contents of the contract. The data referred to in **Annex 1** include those which are also the subject of the referenced contract. This agreement specifies the obligations of the contracting parties under data protection law within the scope of commissioned processing.

§ 1 Subject matter and duration of the order (Art. 28 par. 3)

- (1) The Contractor undertakes to process the personal data specified in more detail in **Annex 1** on behalf of the Customer for the purposes set out therein. The description of the respective order with the information on the subject of the order, scope, type and purpose of the data processing, type of personal data as well as categories of data subjects can be found in the **Annex 1**.
- (2) This agreement begins with the start date of the order and ends with the termination of the contract concluded between the Client and the Contractor. The period for ordinary termination shall be based on the underlying GTC. The right to terminate for cause remains unaffected.
- (3) The Customer may terminate the Agreement at any time without notice if there is a serious breach by the Contractor of the provisions of the GDPR, the Federal Data Protection Act or the State Data Protection Act and other data protection regulations or this Agreement, the Contractor cannot or will not carry out an instruction of the Customer or the Contractor refuses inspections by the Customer or the State Data Protection Officer in breach of the Agreement.

§ 2 Scope, nature and purpose of data processing (Art. 28 par. 3)

- (1) The Contractor shall process the personal data pursuant to Section 1 (1) exclusively within the scope of the order pursuant to Section 1 and in accordance with the Client's instructions. This shall not apply insofar as the Contractor is obliged to process by the law of the EU or the Member States to which the Contractor is subject. In this case, the Contractor shall notify such legal requirements prior to the processing, unless the notification is prohibited by the relevant law due to an important public interest. The Contractor shall not use the data provided for data processing for any other purposes. Copies or duplicates shall not be made without the knowledge of the Client.
- (2) Within this order, the Contractor shall carry out all measures technically required to ensure the purpose of the contract as well as the security and/or processing of the data

(e.g. duplication of inventories for loss protection, creation of log files, etc.), insofar as this processing does not lead to changes in the content of the data and it is necessary for the fulfillment of the order.

(3) The processing of data also by subcontractors takes place

- exclusively in the territory of the Federal Republic of Germany,
- in a Member State of the European Union or in another State party to the Agreement on the European Economic Area,
- in a third country (name of the third country)

takes place. In the latter case, the Contractor shall provide evidence of the lawfulness of the corresponding contractual or other legal basis in accordance with the GDPR. The adequate level of protection in _____.

- is established by an adequacy decision of the Commission (Art. 45(3) GDPR);
- is established through binding internal data protection regulations (Art. 46 (2) (b) in conjunction with Art. 47 of the GDPR);
- is established by standard data protection clauses (Art. 46(2)(c) and (d) GDPR);
- is established by approved rules of conduct (Art. 46 (2) (e) in conjunction with Art. 40 GDPR);
- Is produced through an approved certification mechanism (Art. 46 para. 2 lit. f in conjunction with Art. 42 DSGVO).
- is produced by other measures:

(Art. 46 para. 2 lit. a, para. 3 lit. a and b DSGVO).

Any subsequent transfer to a third country requires prior consent.

§ 3 Technical and organizational measures/security of processing (Art. 28 para. 1, para. 3 c, Art. 32 - 36)

- (1) The Contractor shall take technical and organizational measures (Art. 32 GDPR) to ensure the confidentiality, integrity, availability and resilience of the systems and services in connection with the Processing on a permanent basis. The Contractor shall document the implementation of the technical and organizational measures set out and required in the run-up to the award of the contract before the start of the Processing, in particular with regard to the specific execution of the contract, and shall hand them over to the Customer for review. The Customer is aware of these technical and organizational measures and is responsible for ensuring that they provide an appropriate level of protection for the risks of the data to be processed. The technical and organizational measures of the Contractor are specified separately in **Annex 2** to this Agreement and are part of the contract.
- (2) The Contractor shall ensure to implement a procedure for regular review of the effectiveness of the technical and organizational measures to ensure the security of the Processing.

- (3) The Contractor shall take the technical and organizational measures specified in Annex 2 to this Agreement (pursuant to Art. 32 GDPR) for the processing of personal data within the scope of the order placed by the Customer. The Contractor shall document the implementation of the technical and organizational measures set out and required in the run-up to the award of the contract before the start of the processing, in particular with regard to the specific execution of the contract, and shall hand them over to the Customer for review. The Contractor's technical and organizational measures are set out separately in Annex 2 to this Agreement and form part of the contract. The technical and organizational measures pursuant to Annex 2 to this Agreement have been reviewed by the Customer and assessed as suitable to ensure an appropriate level of protection.
- (4) The Contractor shall ensure the technical and organizational measures required within the scope of the proper execution of the work in cooperation with the subcontractors. The technical and organizational measures of the third parties commissioned by the Contractor shall correspond to the state of the art.

§ 4 Correction, restriction of processing and deletion of data, information about data (Art. 28 para. 1, para. 3g)

The Contractor shall only correct, delete or restrict the processing of data processed under the order on the basis of a provision in the GTC or in accordance with documented instructions from the Client. Insofar as a data subject should contact the Contractor directly for the purpose of correcting, restricting the processing or deleting his/her data, the Contractor shall forward this request to the Client without delay. The same shall apply to requests for information.

§ 5 Controls and other obligations of the contractor (Art. 28 par. 3 h, Art. 32 - 36)

- (1) The Contractor shall ensure compliance with the data protection regulations with regard to the contractual relationship. If the Contractor detects irregularities, it shall immediately inform the Client.
- (2) The Contractor undertakes to maintain confidentiality and any professional secrecy obligations (in particular those protected by Section 203 of the German Criminal Code) when processing personal data of the Client and to provide evidence thereof to the Client. He shall only use employees for the processing who are appropriately obligated and trained. In particular, he shall take due care to ensure that all persons entrusted by him with the processing or performance of this contract are carefully selected, observe the statutory provisions on data protection and do not pass on to third parties or otherwise exploit information obtained from the Client's domain without authorization.
- (3) The Contractor has appointed a data protection officer. His contact details are listed below:

Proliance GmbH / www.datenschutzexperte.de
Datenschutzbeauftragter
Leopoldstr. 2180802
Munich, Germany
datenschutzbeauftragter@datenschutzexperte.de
- (4) The Contractor undertakes to maintain a processing directory in accordance with Article 30 (2) of the GDPR.
- (5) The Contractor undertakes to grant the State Data Protection Officer responsible for the Client and the staff employed by the Client access to the working premises and

submits to control in accordance with the DSGVO, the BDSG and the State Data Protection Acts, if applicable, in their respective form.

- (6) The Contractor shall inform the Customer without undue delay about control actions and measures of the supervisory authority pursuant to the DSGVO, the BDSG and the LDSG. This shall also apply insofar as a competent authority investigates violations at the Contractor.
- (7) If persons whose rights are affected by the data processing at the Contractor contact the Contractor, the Contractor shall immediately refer these persons to the Client. The Customer shall be responsible for safeguarding these rights. The Contractor shall do everything to ensure that the Client can fulfill the rights of the data subjects, in particular to notification, provision of information, correction, restriction of processing (blocking), deletion of data, filing of an objection and the right to data portability, provided that the act of cooperation necessary for the provision of information is not impossible for the Contractor.
- (8) The Contractor shall support the Client in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, data breach notification obligations, data protection impact assessments and prior consultations. This includes, among other things
 - a) Ensuring an adequate level of protection through technical and organizational measures that take into account the circumstances and purposes of the processing, as well as the predicted likelihood and severity of a potential security breach, and allow for the immediate detection of relevant breach events
 - b) The obligation to report personal data breaches to the client without delay
 - c) the support of the client for its data protection impact assessment and
 - d) the support of the client within the framework of prior consultations with the supervisory authority.

§ 6 Subcontracting relationships (Art. 28 par. 2, par. 3 d, par. 4)

- (1) Subcontracting relationships within the meaning of this provision shall be understood to be those services which relate directly to the provision of the main service. This does not include ancillary services which the Contractor uses as services (e.g. as telecommunication services, postal/transport services, user services or the disposal of data carriers) and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. However, the Contractor shall be obligated to enter into appropriate and legally compliant contractual agreements as well as control measures to ensure data protection and data security of the Customer's data even in the case of outsourced ancillary services.
- (2) The conclusion of future subcontracting relationships requires the prior consent of the client.

The outsourcing to subcontractors or the change of the existing subcontractor is permissible insofar as the Contractor notifies the Client of such outsourcing to subcontractors in writing or in text form a reasonable time in advance and the Client does not object to the planned outsourcing to the Contractor in writing or in text form by the time of the notified start of the commissioned processing and a contractual agreement in accordance with Article 28 (2) - (4) of the GDPR is used as a basis. Further outsourcing by the subcontractor requires the express consent of the Principal (at least in text form); such consent is permissible if the subcontractor notifies the Principal of such further outsourcing to subcontractors in writing or in text form a reasonable time in advance and the Principal does not object to the planned further outsourcing to the subcontractor in writing or in text form by the time of the notified start

of the commissioned processing and a contractual agreement in accordance with Article 28 (2) - (4) of the GDPR is used as a basis.

- (3) The transfer of personal data of the Customer to the subcontractor and its first activity shall be permitted only after all requirements for subcontracting have been met. The Customer hereby gives its consent to the commissioning of the subcontractors listed in the GCU - **Annex 3**.
- (4) If the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall ensure that it is permissible under data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of Paragraph 1 Sentence 2 are to be used.
- (5) The Contractor shall impose the same data protection obligations on the subcontractor that it itself has to fulfill vis-à-vis the Client, insofar as this is relevant for the fulfillment of the order. If a subcontractor is engaged, it must be guaranteed that the subcontractor has been carefully selected and that the subcontractor's compliance with the data protection regulations is ensured, that the subcontractor has taken the appropriate technical and organizational measures or will take them until the start of the activity, and that the fulfillment of the Contractor's obligations under this Agreement will not be impaired.
- (6) The Contractor shall be liable to the Customer for data breaches by its subcontractors in accordance with the legal requirements of Art. 28 (4) and Art. 82 - 84 of the GDPR for damages incurred as a result of culpable conduct against the data protection provisions or against this Data Protection Agreement.

§ 7 Control rights of the client (Art. 28 par. 3 h)

- (1) The Customer shall have the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors to be named in individual cases. It shall have the right to satisfy itself of the Contractor's compliance with this Agreement in its business operations by means of spot checks, which must generally be notified in good time. In this context, the Customer shall regularly convince itself of compliance with the technical and organizational measures taken by the Contractor and the subcontractors and document the result. The Customer shall appoint persons responsible for this order control and shall name them to the Contractor in advance. The Contractor shall be informed immediately of any change in the person.
- (2) The Contractor shall ensure that the Customer can satisfy itself of the Contractor's compliance with its obligations pursuant to Art. 28 GDPR. For this purpose, the Contractor shall provide the Customer with evidence of the implementation of the technical and organizational measures pursuant to Art. 32 GDPR upon request. Proof of the implementation of such measures, which do not only relate to the specific order, can also be provided by submitting a current audit certificate or reports. or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors), by compliance with approved codes of conduct pursuant to Art. 40 GDPR or by certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR.
- (3) If the Contractor and/or the subcontractors engaged by it have subjected themselves to approved codes of conduct or have successfully undergone an approved certification

procedure, they shall be obliged to prove this to the Client. Certificates shall be updated. The client shall be informed of this.

§ 8 Notification of violations (Art. 33 par. 2)

- (1) The Contractor shall immediately report to the Client in all cases where the Contractor or the persons employed by the Contractor violate the Client's personal data protection regulations, the confidentiality obligations arising from this Agreement or the stipulations made in the Order.
- (2) In particular, in the case of any existing information obligations in the event of the loss or unlawful transmission of or knowledge gained about personal data pursuant to Art. 33 DSGVO, such incidents must be reported to the Client without delay, regardless of the cause. This shall apply in particular in the event of serious disruptions of the operational process, IT security incidents, suspected violations of regulations for the protection of personal data or other irregularities in the handling of personal data of the Customer. The Contractor shall, in consultation with the Customer, take appropriate measures to secure the data and to mitigate or exclude possible adverse consequences for the data subjects. In particular, if the Customer is subject to obligations based on existing duties to provide information in the event of the loss or unlawful transmission or disclosure of personal data, the Contractor shall support the Customer in this regard.

§ 9 Authority of the Principal to Issue Instructions (Art. 28 Par. 3g, S. 3)

- (1) Data shall be handled exclusively within the framework of the agreements made and in accordance with the client's instructions.
- (2) If the Contractor is of the opinion that an instruction of the Customer violates data protection law, it shall notify the Customer thereof without undue delay. He shall be entitled to suspend the implementation of the corresponding instruction until it is confirmed or changed by the responsible person of the Customer.
- (3) The client's instructions are always given in text form. Verbal instructions are documented in writing.
- (4) The persons listed in Annex 4 shall be authorized to issue instructions on behalf of the Principal. In the case of the Contractor, Florian Kühne or Sven Frauen shall be responsible for accepting instructions. In the event of a change or longer-term prevention of the contact person, the successor or the representative shall be notified to the contractual partner in writing without delay.
- (5) For its part, the Client shall inform the Contractor without undue delay in the event of any errors or irregularities that it discovers, in particular during the examination of results.
- (6) If the Contractor identifies disruptions that require a significant change in the process flow, the corresponding change in the process must be coordinated with the Customer before it is implemented. It may not be carried out without the customer's consent given in text form.
- (7) If the Customer issues individual instructions regarding the handling of personal data that go beyond the contractually agreed scope of services in accordance with the GTC, e.g. changes to the technical and organizational measures, they shall be treated as a request for a change in services, whereby the Contractor does not have to agree to

these and the Customer may have to bear any costs incurred separately insofar as these measures are implemented.

- (8) In the event of a change or long-term prevention of the contact persons, the contract partner must be informed immediately and in principle in writing or electronically of the successors or the representatives. The instructions must be retained for the period of validity and subsequently for three full calendar years.

§ 10 Deletion of data and return of data carriers (Art. 28 Par. 3 g)

- (1) Immediately after completion of the contractual work or earlier upon request by the Client, but no later than upon termination of the cooperation, the Contractor shall hand over to the Client all documents containing personal data that have come into its possession, processing results that have been created, and data files that are related to the contractual relationship, or, with the Client's prior consent, destroy them in accordance with data protection law, generally within 30 days. Exceptions to this are backup copies, which are automatically destroyed 30 days after the deletion of the data, also in compliance with data protection regulations. Within these 30 days, the Contractor shall ensure that the data is stored in a manner that safeguards confidentiality. The protocol of the deletion shall be submitted upon request. A right of retention is excluded.
- (2) Documentation which serves as proof of data processing in accordance with the order and in the proper manner shall be retained by the Contractor beyond the end of the contract in accordance with the retention periods applicable to the service concerned. It may hand this over to the Customer for its discharge at the end of the contract.

§ 11 Final provisions

- (1) Should individual provisions of this agreement be or become ineffective or contain a loophole, this shall not affect the remaining provisions. The parties undertake to replace the invalid provision with a legally permissible provision that comes as close as possible to the economic purpose of the invalid provision or fills this gap.
- (2) Amendments and supplements must be made in writing. This also applies to the amendment of this written form clause.
- (3) Both parties undertake to maintain secrecy about all knowledge gained within the framework of the contractual relationship, in particular about the data that has become known, in compliance with company and business secrecy. This obligation shall continue to apply after the end of the contractual relationship.
- (4) The defense of the right of retention within the meaning of Section 273 of the German Civil Code (BGB) is excluded with regard to the data processed for the person responsible and the associated data carriers.
- (5) If the personal data processed under this agreement at the Contractor are endangered by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Contractor shall inform the Customer thereof without undue delay. The Contractor shall also inform all relevant bodies in this context without delay that the Customer has control over the data.

§ 12 Relationship to GTC

- (1) Insofar as no special provisions are contained in this contract, the provisions of the GTC shall apply.

- (2) In the event of contradictions between this Agreement and provisions from other agreements, in particular from the General Terms and Conditions, the provisions from this Agreement shall take precedence.

Place, date

Berlin

Place, date

Signature, Principal



Signature, Contractor

Annex 1: Description of the processing activity

1. Subject of the order:

Execution of the contractual relationship in accordance with the GTC.

2. Scope, nature (Art. 4 No. 2 DSGVO) and purpose of the data processing:

Implementation of a digital guest management with the possibility for e-mail communication between the organizer and guests, to record online feedback via corresponding websites and to accredit guests at the event location in order to record their attendance. In addition, the data is to be processed for further evaluations with regard to measuring the success of the guest management.

In addition, the data will be processed for the following purposes:

- Transfer of the data of the data subjects by the client to the contractor
- Integration into system/structure of the contractor
- Evaluation by the contractor
- If applicable, integration into sub-websites of the contractor

3. Type of data:

Lfd. No.	Data designation
1	Name, first name
2	E-mail address
3	Company
4	Position
5	Salutation (gender)
6	Title
7	Phone number
8	Other data, the nature of which is determined by the Client and loaded by the Client into the Contractor's system.

No special personal data, i.e. information on racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life are collected, processed and used.

4. Circle of affected persons

Lfd. No	Designation of the persons concerned
1	Employees, trainees, freelancers and other employees of the client
2	Interested parties and customers of the client
3	Employees and/or customers of the Client's business partners in the event of complaints by the business partners against the Client
4	Other visitors/guests/contact persons of the client

Annex 2: Technical and organizational measures

Within the scope of contract processing, MATE Development GmbH (hereinafter referred to as Sweap) undertakes to implement the technical and organizational measures in accordance with Art. 32 DSGVO to the necessary and appropriate extent and in accordance with the generally recognized state of the art within its area of disposal and in relation to the subject matter of the contract. The measures to be implemented by Sweap, oriented to the purpose of the contract, are essentially at least the following:

1. access control

Measures suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data are processed or used.

- secured entrances
- Documentation and regulation of key allocation (allocation of security keys only to permanent employees)
- Door security with safety locks
- Server outsourced: documentation of hoster's security policy, VPN connection between server and company's network

2. access and access control

Measures suitable for preventing data processing systems from being used by unauthorized persons and for ensuring that authorized persons only work on the data processing system within the scope of their authorization.

- Create user profiles
- Authentication with individual user name and individual password
- Documentation of authorizations
- Password policy (16 characters of upper and lower case letters, numbers and special characters for all systems with high security requirements, e.g. access to customer data or Sweap infrastructure)
- Automatic screen lock after 15 minutes of inactivity
- Visitors are only admitted by employees and are only allowed to enter the office premises when accompanied by an employee
- Authorization concept (authorizations according to the "need-to-know" and "need-to-do" principle)
- SSL encryption
- Anti-virus program
- Firewall
- Encryption of data carriers (hard disks) in laptops
- Use of two-factor authentication for other systems (as far as possible)

3. input control

Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered into data processing systems, modified or removed.

- Logging of the entry, modification and deletion of data
- Logging of user activities
- Logging of IT systems (anti-virus, software firewall)
- Regular control of the protocols
- Deletion of the logs after the purpose has been achieved

4. order control

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

- Conclusion of legally compliant data processing contracts according to Art. 28 DSGVO with clients as well as contractors
- Contractually defined responsibilities (person authorized to issue and recipient of instructions)
- Ensuring that personal data of the client are only processed on behalf of the client in accordance with the instruction
- Ensuring the destruction of data after the completion of the order
- Regular control of the TOM of the processors

5. data separation control

Measures to ensure that data collected for different purposes can be processed separately.

- At least factual logical, ideally physical separation according to the purpose of the order
- Separation of the productive and test system by using separate servers and/or server clusters in the ISPs' data center
- No use of live systems for testing purposes
- Compliance with deletion deadlines

6. transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorized persons during electronic transmission or while being transported or stored on data media, and that it is possible to verify and determine to which entities personal data are intended to be transmitted by data transmission equipment.

- WLAN access secured with WPA2
- Encryption on mobile devices via AES-256+SHA2 with a 64-byte encryption key
- Use of VPN with password
- Proper document destruction (use of document shredders with security level P-4 or service providers)
- Proper destruction of data media (use of shredders with security level H-4 or service providers; deletion of data: Overwrite the entire data carrier; for SSD: encrypt from the beginning and overwrite as for other data carriers).

7. data protection through technology design and data protection-friendly default settings

Privacy by Design means "data protection by technical design". The aim is to ensure that suitable technical measures are already implemented during the development of processing operations in order to make the planned processing operations compliant with data protection requirements.

- Sweap's guest management platform requires as little data as possible for an event (variable attributes)
- Event can also be conducted completely anonymously
- Software includes privacy-friendly defaults (e.g., no open rate tracking for emails, no tracking software for guest data logins)

8. availability and resilience (Art. 32 para. 1 lit. b DSGVO)

Measures to ensure that personal data is protected against accidental destruction or loss.

- Regular execution of updates of the anti-virus program
- Locally separated, redundant backup system protected by UPS systems

- Regular test of data recovery from backups
- Monitoring the system load
- Regular random performance checks by backing up the Data

9. organizational control

These are measures that ensure that employees are informed about and sensitized to the requirements of data privacy and that they are obligated to comply with data privacy. In addition, the point of organization includes overarching concepts in which the company management specifies how it intends to handle data protection in the company.

- Demonstrable commitment of all employees to confidentiality (data secrecy), if applicable to telecommunications secrecy and the maintenance of professional secrecy
- Corporate concepts for data protection and data security
- Employee training on data protection and data security
- IT contingency plan, the functionality of which is regularly tested and documented.
- Home Office Policy
- Regulation on the use of company e-mail and Internet access in the employment contract
- Documentation of the IT systems used and their system configuration
- Permanent and lived reminder to all employees on how to deal with data protection-critical content

10. effectiveness control

All actions that lead to evidence that the measures used are regularly reviewed and actually work.

- Regular monitoring of the technical and organizational measures implemented
- Regular control of the authorizations granted to employees
- Regular control of the functioning of anti-virus systems and firewalls

Annex 3: Subcontractors or sub-subcontractors

The contractually agreed services or the partial services described below shall be performed using the following subcontractors or sub-subcontractors:

Description of partial services (not conclusive)	Name and address of the subcontractor
Hosting	<p>IBM Deutschland GmbH (Platform-as-a-Service Provider / Hosting) IBM-Allee 1, 71139 Ehningen, Germany Post address: 71137 Ehningen, Germany</p> <p>Data center locations: Frankfurt (Germany)</p>
Hosting	<p>Hetzner Online GmbH (DNS and domain hosting): Service provider in the sense of § 5 TMG: Industriestr. 25, 91710 Gunzenhausen, Germany</p> <p>Data center locations: Nuremberg, Falkenstein (Germany)</p>
Hosting	<p>hosting.de GmbH (DNS and domain hosting): Franzstr. 51, 52064 Aachen, Germany</p> <p>Data center locations: Aachen, Cologne, Nuremberg (Germany)</p>
Cloud solution	<p>Mailjet (Email Service Provider): Mailjet SAS (Global HQ) 13-13 bis, rue de l'Aubrac, 75012 Paris, France</p> <p>Mailjet GmbH Postal and invoice address: Alt-Moabit 2, 10557 Berlin, Germany Registered office: Rankestr. 21, 10789 Berlin, Germany</p> <p>Data center locations: Frankfurt (Germany), Saint-Ghislain (Belgium)</p>

Annex 4: Persons authorized to issue instructions on behalf of the Principal

Lfd. No	Designation of the persons authorized to issue instructions
1	Management Board
2	The data protection officer(s) appointed by the client