Terms of Service

Meisterplan Software as a Service Terms and Conditions

Last Updated: November 7, 2023

Meisterplan Software as a Service Terms and Conditions (hereinafter referred to as **"Terms of Service"**) to an agreement entered into via the Meisterplan Webshop or in any other way (hereinafter referred to as **"Agreement"**) between itdesign GmbH, Friedrichstrasse 12, 72072 Tübingen, Germany (hereinafter referred to as the **"Supplier"**) and you or the company/organization that you represent (hereinafter referred to as the **"Customer"**), hereinafter collectively referred to as the "Parties".

These Terms of Service are composed of

- the following terms and conditions for the provision of the Services by the Supplier (Part I) (hereinafter referred to as the **"Service Contract"**) and
- the Agreement on Data Processing between the Parties (Part II) (hereinafter referred to as the **"Data Processing Agreement"**).

Part I – Service Contract

1 Subject of the Agreement, definitions

(1) Under the Agreement, the Parties agree that the Supplier is to give the Customer the right, subject to a fee, to use the software application "Meisterplan" (referred to hereinafter as the **"Application"**).

(2) The subject of the Agreement is the provision by the Supplier to the Customer, subject to payment of the fee for the term agreed in the Agreement or in a separate agreement, of the current version of the Application made available by the Supplier for the use of its functionalities, the technical facility to use the Application and the grant or transfer of rights of use to the Application.

(3) A functional description of the Application is available for download at https://www.meisterplan.com/wp-content/uploads/meisterplan-product-description.pdf

The software environment approved by the Supplier for use of the Application, in particular the browser, is specified in the Application system requirements and is available for download at https://www.meisterplan.com/wp-content/uploads/meisterplan-system-requirements.pdf

(4) Resource: A **“Resource”** means, hereinafter, an individual person or material resource that you plan for using the Application. Each resource may also log in as a user of the Application. If the customer uses “placeholder”, “proxy-resources” or roles, one resource must be licensed for every represented person or material resource.

Environment: An **“Environment”** is a logical unit on which the Application is operated. This may be a physical or virtual server; which can be accessed with the aid of a browser.

2 Provision of the Application, securing the Application Data

(1) The Supplier shall keep the latest version of the Application on a central data processing system or several data processing systems (referred to hereinafter as **“Server“**, even if there are several of them), in accordance with the following provisions.

(2) The Application and the data entered by the Customer into the Application (hereinafter the **“Application Data”**) shall be backed up regularly on the Server, at least once daily, unless agreed otherwise between the Parties. The security backup generated shall be filed on the Server. The backup thus filed shall be held for thirty (30) days before being automatically overwritten on the following working day.

(3) The point of delivery of the Application and the Application Data shall be the router output of the data processing center used by the Supplier (referred to hereinafter as the **“Delivery Point“**).

(4) If you are a Competitor, defined as an individual or an entity engaged in a business that provides products or services substantially similar to Meisterplan's offerings, including agents, employees, or representatives, you are expressly forbidden from accessing or using the Application. This prohibition extends to signing up for free trials. Additionally, you may not access the Application for purposes of monitoring its availability, performance, or functionality, or for any other benchmarking or competitive purposes. Violation of this clause may result in immediate termination of your access to the Application and may subject you to legal action.

3 Application trial versions

The Customer has the opportunity to test the Application free of charge. The free trial version of the Application shall be provided to the Customer solely for trial purposes for a limited period. A trial version is not permitted to be used for normal business operations.

The Application Data shall be deleted automatically 30 days after the end of the trial phase.

4 Service levels

This paragraph sets the general service levels for the use of the Application.

(1) Technical availability of the Application

a) The Supplier shall make the Application available to the Customer during the following System Runtime, with the exception of the agreed scheduled outage periods pursuant to Clause 4 (2) below.

The **“System Runtime”** shall be 24 hours a day and 365 days a year.

b) The parties agree to the periods of available use (which means availability exists) as follows: Within the System Runtime, a Primary Processing Time is defined during which the Supplier ensures monthly availability of the Application from Monday to Friday from 09.00 – 17.00 CE(S)T to 99%. During this time, the longest uninterrupted downtime will not exceed 4 hours.

All times outside the Primary Processing Time are considered as Secondary Processing Time during which availability is not ensured. Primary Processing Time excludes Saturdays, Sundays, January 1 and December 25.

c) The Application will be deemed to be available during periods of time in which

- The Application cannot be accessed (or other faults exist) due to problems with the local IT system of the Customer, or in a fault in the Customer’s connection to the Server, or
- other events occur, which are not caused by the Supplier or its agents, e.g., due to force majeure, abuse or operator error.

(2) Scheduled outages

Supplier may schedule outage periods in order to service and maintain the Application and/or Server, and to perform other tasks. The Supplier will announce scheduled outages to the Customer no less than 7 days in advance at https://status.meisterplan.com.
Even if the Customer is able to use the application during the scheduled outage period, it shall not be legally entitled to do so. If, during use of the Application during scheduled outage periods, there is a reduction in performance or suspension of performance, the Customer may not make a claim for liability for defects or for damages.

(3) Measuring actual availability

The actual availability percentage for Primary Processing Time is calculated as follows:

$$\frac{\textit{period of actual availability during the Primary Processing Time in seconds}}{\textit{length of the Primary Processing Time during the month in question in seconds}} * 100$$

The availability shall be determined by a monitoring instance of the Supplier. The availability of the Application itself as well as that of the application services (such as reporting) shall be monitored.
Based on this monitoring procedure, data on availability shall be automatically generated, which the Supplier makes available to the Customer at https://status.meisterplan.com

(4) Response times

The Supplier shall ensure, within the Primary Processing Time only, that fault rectification work shall begin within a period agreed below, based on the respective fault class defined below, following receipt of a report of a technical fault from the Customer by e-mail or support ticket (**”Response Time”**).

In the case of faults reported outside the Primary Processing Time, the Response Time shall start on the next business day within the primary processing time.

Fault class	**Response Time**
Fault class 1	4 hours
Fault class 2	2 business days
Fault class 3	5 business days

The fault classes are defined as follows:

Class 1: Defect that prevents operation
A defect that prevents operation shall exist if use of the Application is impossible; a workaround is not available.

Class 2: Defect that hinders operation
A defect that hinders operation shall exist if use of the application is significantly restricted and no workaround is available.

Class 3: Minor defect
A minor defect shall exist if use of the application is possible without restriction or with minor restrictions.

(5) Breach of availability and remedy

If, during the Primary Processing Time, the Supplier does not meet the availability targets set out under Clause 4 (1), the Customer shall be entitled to demand payment of a contractual remedy (referred to hereinafter as **“Service Level Credit“**) as follows:

- if the availability during the Primary Processing Time is not achieved: 0.5% of the monthly fee (pro rata) per failure, by 0.1% or part thereof, to achieve the agreed availability, albeit up to a maximum of 100% of the monthly fee;

- if the longest uninterrupted downtime is overrun during the Primary Processing Time: 5% of the monthly fee (pro rata) per overrun, albeit up to a maximum of 100% of the monthly fee;

- if Supplier does not meet the Response Time targets for a Fault Class 1 issue during Primary Processing Time: 5% of the monthly fee (pro rata) per overrun, albeit up to a maximum of 100% of the monthly fee.

This will not apply if the Supplier is not responsible for the failure to achieve the availability/for the overrun of the downtime/reaction time. The value of the total Service Level Credits owed to Customer will be paid out to the Customer or offset against current invoices from the Supplier.

The Service Level Credits shall be credited against any claims for damages by the Customer. Apart from claiming Service Level Credits, the Customer may require the Supplier to continue to fulfil the Agreement.

5 Other services of the Supplier, online user manual

(1) The Supplier shall provide the Customer with new versions of the Application developed during the Agreement term (in particular updates, upgrades or releases). The new versions may also contain extended functionalities.
The Customer shall not have the right to require new versions to be produced or to demand the inclusion of specific additional functionalities in the Application.

(2) The Supplier shall provide the Customer with an online user manual for the Application.

6 Rights of use, rights of the Supplier in the event that rights of use are exceeded

(1) The Customer shall receive a simple, non-exclusive right of use for the Application, which may not be the subject of a subsidiary license and shall be non-transferable, shall be limited in time to the term of the Agreement in accordance with these Terms of Service.

The Customer may only use the Application for its own commercial activities involving its own staff or agents, including staff or agents from affiliated companies.

(2) The Customer may only use the Application according to the number of resources stated in Clause 1 (4) of this Service Contract.

(3) The Customer shall have access to one (1) environment. No additional environments will be provided for testing or quality assurance purposes. These may be ordered as required for an additional charge.

(4) The Customer shall have no rights other than those explicitly granted to it above. In particular, the Customer shall not be entitled to use the Application beyond what is agreed or to allow its use by third parties, or to make the Application accessible to third parties.

(5) If the Customer does not comply with the obligations under Clause 6 (1) to (4) of this Service Contract, the Supplier may block the Customer’s access to the Application or the Application Data, if this demonstrably prevents continuation of the noncompliance.

If, despite a written warning by the Supplier, the Customer continues the noncompliance described under Clause 6 (1) to (4) of this Service Contract, or is responsible for their continuation or repetition, the Supplier may terminate the Agreement for cause without notice.

7 Fee and payment

(1) The Customer shall pay the Supplier the fee for use shown in the Agreement, plus any required value added tax at the statutory rate, for the services to be provided, namely granting use of the Application.

(2) The fee is due for payment in advance of service at the times set out in the Agreement.

(3) The Supplier shall be entitled to reasonably increase the agreed upon prices for the contractual services in order to meet staffing costs and other cost increases. The Supplier shall notify the Customer of a price increase in writing or via email; the price increase shall not apply to the period for which the Customer has already made payments.

The prices may not be increased within 12 months of the effective date of conclusion of the Agreement.

(4) If entering into a paid Agreement (thus the exception of trial versions), the Customer hereby grants to the Supplier the right to use the Customer's company logo in marketing materials such as the Supplier's website solely to identify the Customer as a Meisterplan customer. This permission may be revoked informally by sending an e-mail to mail@meisterplan.com. The Supplier shall not use the Customer's logo without prior written permission in any other manner.

8 Customer's duties of cooperation

(1) The Customer shall fulfill all duties and obligations that are required in order to process the Agreement. The Customer undertakes in particular:

1. not to disclose the use and login credentials assigned to it or the users, to prevent them from being accessed by third parties and not to pass them to unauthorized users;
2. to protect the user IDs, passwords and the like through appropriate and customary means; the Customer shall notify the Supplier promptly in the event of any suspicion that the access data and/or passwords may have become known to unauthorized third parties;
3. to adhere to the restrictions/obligations in relation to the rights of use set out in Clause 6 of this Service Contract; and in particular:
    - not to retrieve or allow retrieval of any information or data without authorization, or to interfere with or allow interference with programs operated by the Supplier, or to infiltrate or promote infiltration into the Supplier's data networks without authorization;
    - to indemnify the Supplier in the event of claims by third parties that result from the unlawful use of the Application by the Customer, or that arise out of disputes under data protection law, copyright law or other legal disputes brought about by the Customer, which are associated with the use of the Application;
    - to require authorized users to also adhere to the provisions of the Agreement and of these Terms of Service that apply to them;

- to inform the authorized users of the processing of their personal data by the Supplier in accordance with Art. 13 and 14 GDPR.

4. to check data and information for viruses before sending them to the Supplier and to install state-of-the-art antivirus software;

5. to promptly declare to the Supplier any defects in the contractual services, in particular defects in the services described in Clause 1 of this Service Contract;

9 Data security, data protection

(1) The Parties shall observe the data protection provisions applicable to them, in particular those that are valid in Germany, including Regulation (EU) 2016/679 (General Data Protection Regulation).

(2) If the Customer gathers, processes or uses personal data, it shall be answerable for the fact that it is entitled to do so under the applicable legal provisions, in particular those under data protection law, and shall indemnify the Supplier for claims by third parties in the event of a breach of such provisions.

(3) Within the framework of the implementation of this Agreement, a distinction shall be made between the following categories of data, some of which may contain personal data:

1. The Supplier processes personal data of the Customer’s contact persons (contact person, address, telephone number, fax, e-mail address) for the performance of the contract, in particular within the scope of the billing. This data is processed on the basis of legitimate interests pursuant to Art. 6 Para. 1 Letter b) GDPR. The purpose of the processing is to implement the Agreement with the Customer. Information on the rights of the data subject and deadlines for deletion can be found in the Supplier’s data protection information, which can be viewed at https://www.meisterplan.com/privacy-and-data-protection/.

2. The Supplier processes data on the usage behavior of the Customer’s users within the framework of server protocols which may contain information such as IP address, time stamp or web inquiry. This data is processed on the basis of legitimate interests pursuant to Art. 6 Para. 1 Letter f) GDPR. The purpose is, on the one hand, to search for and rectify errors, to avert threats to security, and to maintain the technical operation of the application. Information on the rights of the data subject and deadlines for deletion can be found in the Supplier’s data protection information, which can be viewed at https://www.meisterplan.com/privacy-and-data-protection/.

3. The Supplier processes statistical data for the use of the Application. This data does not include any content that users have entered in the Application. The data may include actions triggered by the user, a time stamp, information on the web browser used, the internal ID of the respective database, an ID of the session, a non-invertible user ID, or the ID of a cookie generated on the website. These data are processed on the basis of legitimate interests in accordance with Art. 6 Para. 1 letter f) GDPR. The purpose of the processing is the continued provision of the service, the adaptation to the developing needs of the users, the improvement of the user experience in the application, and the optimization of

the internal processes of the Supplier. Information on the rights of the data subject and deadlines for deletion can be found in the Supplier's data protection information, which can be viewed at https://meisterplan.com/privacy-and-data-protection/.

4. The Supplier ultimately processes Application Data, i.e. the data entered by the Customer during use of the Application. This data is processed on behalf of the Customer in accordance with Art. 28 GDPR under the Data Processing Agreement (Part II of these Terms of Service).

(4) The obligations set out in Clause 9 (1) to (3) of this Service Contract shall apply for as long as the personal data remain within the Supplier's range of influence, including beyond the end of this Agreement.

(5) The Supplier is entitled to use subcontractors in order to provide its services. A continuously updated list of the subcontractors used by the Supplier to process personal data on its behalf, can be viewed at https://meisterplan.com/subcontractors/. Insofar as the Supplier entrusts subcontractors with the processing of the Customer's personal data, of which the Supplier processes as a processor pursuant to Art. 28 GDPR, the special provisions of the Data Processing Agreement (Part II of these Terms of Service) shall apply. Such subcontractors will be included in a separate list.

(6) The Customer shall be responsible for the content that has been uploaded during use of the Application, and shall regularly prepare its own backups, in order to permit reconstruction of the content in the event of loss of the data and information.

(7) If and insofar as the Supplier provides the Customer with the requisite technical facilities to do so, the latter shall regularly download backups for the Application Data stored on the Server.

10 Claims in the event of defective performance

In the event of defective performance, the Customer shall be entitled to the claims according to Clause 4 of this Service Contract (Service levels). In all other respects the statutory provisions shall apply.

11 Confidentiality

(1) The Parties mutually agree to treat all knowledge of business secrets and other confidential information of the respective other party acquired within the scope of the contractual relationship as confidential, and to use such information exclusively for the purposes of implementing the Agreement.

(2) This obligation shall remain in force even after termination of this Agreement.

12 Liability

The liability of the Supplier is governed by law.

13 Proprietary rights of third parties

(1) The Supplier hereby guarantees that the Application is free from industrial property rights and copyrights of third parties.

If a third party asserts justified claims against the Customer owing to the infringement of proprietary rights by the Supplier's Application, the Supplier shall be liable towards the Customer as follows:

1. The Supplier shall, at its own discretion and at its own expense, either obtain a right of use for the Application or the relevant part of the Application, or change the Application in such a way that the proprietary right is not infringed, or exchange the Application. If it is not possible for the Supplier to do so under reasonable conditions, then the Customer may avail itself of the statutory rights to withdraw from the Agreement or demand a reduction.
2. In the event of a legitimate claim being made against the Customer by a third party, the Supplier shall release the Customer from the costs that have arisen through the raising of these third-party claims (including reasonable lawyers' fees, which shall be limited, where applicable, in accordance with the Rechtsanwaltsvergütungsgesetz (German Law on the Remuneration of Attorneys).
3. The Supplier's obligation to pay damages is based on Clause 12 of this Service Contract.

The Customer undertakes to notify the Supplier promptly, in writing or by e-mail, of the claims being asserted by third parties; the Supplier reserves the right to take all defensive measures and to conduct settlement negotiations. If the Customer discontinues use of the Application in order to reduce the damage for other important reasons, it shall be obliged to point out to the third party that the discontinuation of use does not constitute acknowledgement of an infringement of a proprietary right.

(2) Claims against the Supplier in accordance with Clause 13 (1) of this Service Contract shall be excluded if

1. the Customer is responsible for the infringement of the proprietary right,
2. the assertion of an infringement comes about through unauthorized modification of the Application by Customer or is associated with such a modification,
3. the Application is not used in accordance with the provisions of the Agreement and of these Terms of Service or in accordance with the Application documentation.
4. the alleged infringement could have been prevented through the use of an update, upgrade or patch released by the Supplier,
5. the alleged infringement results from the use of the Application with a product from a third-party supplier that has not been made available by the Supplier.

(3) Further claims of the Customer against the Supplier and its vicarious agents owing to claims resulting from the infringement of proprietary rights of third parties are excluded.

14 Entering into the Agreement, start of the Agreement, term, termination

(1) The Customer makes an order by clicking the button “Order Now” on the Meisterplan Webshop or through other forms of communication.

The Agreement is executed and the contractual relationship shall commence with the acceptance of the Customer`s order by order confirmation of the Supplier.

(2) The Agreement shall have the minimum term as agreed in the Agreement and may not be the subject of ordinary termination prior to that point.
The Agreement shall be extended by further periods of the originally agreed term unless terminated by one of the Parties at the end of the minimum term or the extension period in question. The Parties may agree in writing upon a different notice period for termination of the Agreement.

(3) This shall not affect the right of the Parties to terminate the Agreement for cause.

15 Duties during and after the end of the Agreement

When the contractual relationship ends, all the Customer’s rights to use the Application shall lapse. The Supplier shall delete the Customer’s Application Data no later than 30 days after the end of the Agreement.

16 Force majeure, delays in performance of the service

The Supplier shall not be liable for delays in performance of the service due to force majeure, which shall include events that make it significantly more difficult or impossible for the Supplier to perform the services under the Agreement, including in particular strike, lockout, official orders, failure of, or problems associated with, communication networks and gateways of other operators, inasmuch as the Supplier was not responsible for such events.

Such events shall entitle the Supplier to postpone or interrupt the services for the duration of the hindrance.

17 Final provisions, place of jurisdiction, governing law

(1) All agreements, ancillary agreements and assurances, as well as subsequent amendments and supplements to the Agreement and/or these Terms of Service require a corresponding agreement between the Parties.

(2) If a provision of the Agreement and/or of these Terms of Service is or becomes ineffective or is incomplete, this shall not affect the remainder of the Agreement; the remaining provisions shall remain effective.

In such a case, and in the case of loopholes that the Parties have not foreseen, the Parties shall agree on a provision that best fulfills the intent and purpose of the Agreement and these Terms of Service and that reflects those of the invalid provision as closely as possible.

(3) The Agreement and these Terms of Service shall be governed by the law of the Federal Republic of Germany, to the exclusion of the UN Convention on Contracts for the International Sale of Goods (CISG).

(4) The place of performance and exclusive place of jurisdiction for all disputes arising out of or in connection with the Agreement and/or these Terms of Service shall be Tübingen, Federal Republic of Germany.

Part II – Data Processing Agreement

1 Scope of application

(1) The parties agree that the Supplier shall act as a processor for the Customer when providing the services, insofar as the Supplier processes Application Data for the Customer (cf. the definition of Application Data in Clause 2 (2) of the Service Contract (Part I of these Terms of Service).

(2) It is noted that the Supplier can process personal data of the Customer which are not the subject of this Data Processing Agreement, since the Supplier acts as a Controller in this respect. This concerns, for example, data for billing and license management, or automatically collected statistical data. For details, reference is made to the provisions in Clause 9 (3) of the Service Contract (Part I of these Terms of Service). It is ensured that this data is kept separate from the Application Data provided for processing. In addition, reference is made to the Supplier's data protection information.

2 Subject of the Data Processing Agreement

The Supplier will process personal data for the Customer within the meaning of Art. 4, Cl. 2 and Art. 28 of the General Data Protection Regulation (GDPR) for purposes of this Data Processing Agreement.

3 Duration of the Data Processing Agreement

(1) The term of this Data Processing Agreement corresponds to the duration of the Agreement.

(2) The Customer may terminate the Agreement at any time without notice if the Supplier commits a serious breach of this Data Processing Agreement, the Supplier cannot or does not want to carry out instructions from the Customer, or the Supplier refuses to honor the contracting rights of the Customer stipulated within this Data Processing Agreement.

4 Type and purpose of processing, type of personal data, and categories of affected persons

(1) The subject of this Data Processing Agreement is personal Application Data which the customer enters into the Application in order to manage it there.

(2) The type of processed personal Application Data is basically determined by the Customer. Meisterplan offers the entry of first name, last name, e-mail address, role, start and end of employment, postal code and city (no personal address), skills and project planning. The Customer is obliged not to enter any special categories of personal data in the Application.

(3) Typically, the data subjects are internal employees, external employees, and suppliers of the Customer. The Customer determines the categories of data subjects at the time of data entry. In principle, data of all categories of data subjects can be processed.

5 Rights and obligations as well as authority of the Customer

(1) The Customer alone is responsible for the assessment of the permissibility of data processing in accordance with Art. 6, Para. 1 of the GDPR as well as for the protection of the rights of the data subjects in accordance with Art. 12 to 22 of GDPR. Nevertheless, the Supplier is obliged to promptly forward all such requests to the Customer if they are clearly directed to the Customer alone. Changes to the type of data that is processed and changes to procedure must be coordinated jointly by the Customer and the Supplier, and they must be defined in writing or in an electronic format.

(2) The Customer usually issues all orders, partial orders, and instructions in writing or in an electronic format. Verbal instructions must be confirmed promptly in writing or in an electronic format.

(3) The Customer may request proof that the Supplier’s technical and organizational measures comply with the obligations set out in this Data Processing Agreement before the start of processing under this Data Processing Agreement and thereafter at regular intervals within reason.

(4) The Customer informs the Supplier promptly if it finds any errors or irregularities during the validation of any data processing results.

6 Obligations of the Supplier

(1) The Supplier will process the personal Application Data provided for processing only in accordance with the agreements and instructions of the Customer, unless it is required to process this data in a different way under a European Union or member state law to which the Supplier is subject as a data processor (e.g., as required by investigations by law enforcement or state protection authorities); in such a case, the Supplier will inform the Customer of these legal requirements prior to processing, unless the law prohibits such communication because of an important public interest (Art. 28, Para. 3, Cl. 2 (a) of the GDPR).

(2) The Supplier will not use the personal Application Data provided for processing under this Agreement for any other purpose, and in particular for its own purposes. Copies or duplicates of this Application Data may not be produced without the knowledge of the Customer.

(3) The Supplier guarantees that the Application Data that is processed for the Customer will be kept strictly separate from other data.

(4) In respecting the rights of data subjects in accordance with Art. 12 to 22 of the GDPR on behalf of the Customer, and when preparing the lists of processing measures as well as when the Customer performs required data protection follow-up assessments, the Supplier must cooperate to the extent necessary to support the Customer as much as reasonably possible (Art. 28, Para. 3, Cl. 2(e) and (f) of the GDPR).

(5) The Supplier must inform the Customer without delay if, in its opinion, an instruction issued by the Customer violates statutory provisions (Art. 28, Para. 3, Cl. 3 of the GDPR). The Supplier may suspend the execution of the relevant instruction until it has been confirmed or changed by the Customer after verification of the Supplier's objections.

(6) The Supplier will amend, cancel or restrict the processing of personal Application Data resulting from the Data Processing Agreement if the Customer so requests by issuing an instruction and the legitimate interests of the Supplier are not violated by this instruction.

(7) The Supplier may only disclose personal Application Data that are subject to this Data Processing Agreement to third parties or data subjects after prior instruction or approval by the Customer.

(8) The Supplier agrees that the Customer is entitled (on the basis of an advance appointment) to monitor compliance with the provisions on data protection and data security as well as the contractual agreements to the appropriate extent and as required by third parties commissioned by the Customer, in particular by obtaining Information and access to the Supplier's stored Application Data and the data processing programs as well as on the basis of inspections (Art. 28, Para. 3, Cl. 2(h) of the GDPR).

(9) The Supplier warrants that it will assist, as necessary, in observing these controls.

(10) The Supplier undertakes to maintain confidentiality when processing the Customer's personal data processing of Application Data under this Data Processing Agreement. This provision will remain in force after the end of the Agreement.

(11) The Supplier warrants that it will inform its employees that will carry out data processing of the relevant data protection provisions before commencing their work on processing data under this Data Processing Agreement, and that it will commit them to maintaining confidentiality of the data during their employment as well as after the termination of their employment relationship (Art. 28, Para. 3, Cl. 2 (b) and Art. 29 of the GDPR).

(12) The Supplier will monitor compliance with the data protection regulations at its company.

(13) The currently appointed Data Protection Officer can be viewed at https://www.meisterplan.com/privacy-and-data-protection/.

7 Reporting obligations of the Supplier in case of processing delays and personal data breaches

(1) The Supplier will promptly notify the Customer of any disruptions, violations of the data protection provisions or the stipulations specified in this Data Processing Agreement that are committed by the Supplier or persons who are employed by it, as well as of suspected data breaches or irregularities in how personal Application Data has been processed.

(2) This also applies in particular to any notification and reporting obligations of the Customer in accordance with Art. 33 and Art. 34 of the GDPR. The Supplier undertakes to provide the Customer with appropriate support to carry out its duties under Art. 33 and 34 of the GDPR (Art. 28, Para. 3, Cl. 2 (f) of the GDPR).

(3) The Supplier may only send notifications as defined in Art. 33 or 34 of the GDPR on behalf of the Customer in accordance with prior instructions.

8 Subcontracting relationships with subprocessors (Art. 28. Para. 3, Cl. 2(d) of the GDPR)

(1) The Supplier may only hire subprocessors to process Application Data at the express permission of the Customer (Art. 28, Para. 2 of the GDPR). The Supplier must ensure that it carefully selects its subprocessor while ensuring that the subprocessor has taken appropriate technical and organizational measures within the meaning of Art. 32 of the GDPR.

(2) Depending on the location from which the Customer registers, the Supplier decides on the data center location. Application Data of customers whose IP address indicates an EU location will be hosted at a location within the EU or EEA. For all other locations, the Supplier reserves the right to freely determine the location of the data center, including the right to process the data in the USA or other third countries.
The hiring of subprocessors, or additional processing of the Customer's personal data, is only allowed in third countries if the special requirements of Art. 44 et seq. of the GDPR are met.

(3) The Supplier shall ensure that the agreed upon regulations between the Customer and the Supplier also apply to subprocessors to the extent that a level of protection corresponding to the GDPR is guaranteed. The parties make it clear that this does not imply any obligation on the part of the Supplier to impose the provisions of this Data Processing Agreement on the subprocessor in the same wording. If several subprocessors are used, this shall also apply to the responsibilities between these subprocessors.

(4) The agreement with the subprocessor must be made in writing, though it may be made in an electronic format (Art. 28, Para. 4 and Para. 9 of the GDPR).

(5) Data may only be forwarded to the subprocessor if the subprocessor has fulfilled the obligations stipulated in Art. 29 and Art. 32, Para. 4 of the GDPR with regard to its employees.

(6) The Supplier will be liable to the Customer for ensuring that its subprocessor complies with the data protection obligations that are contractually imposed by the Supplier in accordance with relevant sections of the Data Processing Agreement.

(7) The current list of the Supplier's subprocessors is available at https://meisterplan.com/subprocessors/. The Customer agrees to their employment.

(8) In accordance with Art. 28. Para. 2, Cl. 2 GDPR, the Supplier may hire additional subprocessors. In this case, the Supplier shall inform the customer by e-mail 30 days before data is shared with the subprocessor. After this period the new list of subprocessors will be made available at https://meisterplan.com/subprocessors. In this respect, it should be made clear that the Customer will be informed only if subprocessors are hired who have access to the Customer's personal data.

(9) In case the Customer reasonably objects to the appointment of another sub-processor within 30 days upon receipt this information, the parties will come together in good faith to discuss an appropriate solution. If such solution can not be reached, the Customer may terminate the Agreement and shall receive a pro-rated refund of prepaid unused fees.

9 Technical and organizational measures in accordance with Art. 32 of the GDPR (Art. 28, Para. 3, Cl. 2(c) of the GDPR)

(1) An adequate level of protection is provided to counteract the risks to the rights and freedoms of persons whose data is processed during the course of processing of data under this Data Processing Agreement. For this purpose, the protection objectives of Art. 32, Para. 1 of the GDPR, including confidentiality, integrity, and ensuring the availability of the systems and services and their resilience with regard to the type, scope, circumstances, and purpose of the processing are taken into account when choosing appropriate technical and organizational corrective measures that permanently reduce risk.

(2) Appendix 1 ("Technical and Organizational Measures") lists the Supplier's technical and organizational measures.

(3) The measures that are taken by the Supplier may be subjected to further technical and organizational refinement in the course of the performance of the Data Processing Agreement, but they must not fall short of the agreed standards.

(4) The Supplier and the Customer must agree upon any significant changes in documented form (in writing or electronically), insofar as these changes affect the provision of the service. Such coordination must be maintained for the duration of this Data Processing Agreement.

10 Obligations of the Supplier after the completion of processing of data under this Data Processing Agreement (Art. 28, Para. 3, Cl. 2(g) of the GDPR)

(1) After completion of processing of Application Data under this Data Processing Agreement, the Supplier must delete all Application Data that the Customer transferred for processing.

(2) This is achieved by configuring the automatic deletion of the Application Data upon the expiration of thirty (30) days after the termination of the contractual relationship. For details, reference is made to the provisions of Clause 14 of the Service Contract (Part I of these Terms of Service).

11 Liability

Please refer to Art. 82 of the GDPR.

Appendix 1: Technical and Organizational Measures

The following technical and organizational measures are carried out by the Supplier in the Meisterplan division.

Access control

1. Every user access to data processing equipment and systems is only possible via user authentication using a password or through a Single-Sign-On (SSO) solution.
2. Password Policy as per Active Directory Policy.
3. Access to the central Customer Relationship Management System is linked to the employee’s user account via SSO technology.
4. Levels of user access are managed and created by assigning user privileges.
5. Computer screens are locked after 5 minutes of inactivity as per the user policy.
6. VPN access granted to selected employees working from outside the company network.
7. Chip card locking system and security locks.
8. Allocation, collection, and blocking of chip cards are all centrally controlled.
9. Access control at the reception desk.
10. Each building level is separately secured by chip card access.
11. Guest cards.
12. The vehicle and pedestrian entrances to the underground garage are kept under video surveillance.
13. The pedestrian entrance to the Supplier’s underground garage is secured with an alarm system.

14. Server rooms may only be accessed by IT department employees and company executives, and the entrances to these areas are specially secured.

In addition to the above mentioned measures, the Meisterplan division also carries out the following measures for the Customer:

1. Two-factor authentication is used for password management software and the AWS hosting provider.
2. Only secure passwords are allowed for applications, and these are managed using password management software.
3. Administrative access to the AWS console is logged.

For the security guidelines of the AWS Computing Center, see: : https://aws.amazon.com/compliance/data-center/controls/

Data storage media control

1. Employees who work in public places use screen protectors on their laptops.
2. Clean desk policy.
3. The hard drives of notebooks/laptops are encrypted.

In addition to the above mentioned measures, the Meisterplan division also carries out the following measures for the Customer:

1. At Meisterplan no data storage media are sent to third parties or received from third parties. All data is exchanged using a file-sharing platform that utilizes an access rights and deletion concept and is accessible using a secure connection.
2. The use of USB sticks to process customer data is not allowed at Meisterplan.

Storage control

1. Every user access to data processing equipment and systems is only possible via user authentication using a password or through a SSO solution.
2. Access to the central Customer Relationship Management System is linked to the employee's user account via SSO technology.
3. In the central Customer Relationship Management System access to the system and data changes are logged.
4. The changes to user authorizations in the central Customer Relationship Management System are manually logged in the administration interface.

5. Levels of user access are managed and created by assigning user privileges.

6. Workstation computer screens are locked after 5 minutes of inactivity as per the user policy.

In addition to the above mentioned measures, the Meisterplan division also carries out the following measures for the Customer:

1. Test data is stored separately from production data. Specifically, this means that the Meisterplan Continuous Integration Cluster is kept separate from the Production Cluster.

2. Meisterplan Application Data backups are only transported/stored in an encrypted state. The backups are stored in the respective region (USA/Germany).

3. Application Data may only be used with the consent of the Customer for error reproduction or consulting purposes. Data copies will be permanently deleted after the task that required use of this data has been completed.

4. When data is transferred, it is always encrypted.

User control

1. Every user access to data processing equipment and systems is only possible via user authentication using a password or through a SSO solution.

2. Access to the central Customer Relationship Management System is linked to the employee’s user account via SSO technology.

3. In the central Customer Relationship Management System access to the system and data changes are logged.

4. The changes to user authorizations in the central Customer Relationship Management System are manually logged in the administration interface.

5. Levels of user access are managed and created by assigning user privileges.

6. Workstation computer screens are locked after 5 minutes of inactivity as per the user policy.

In addition to the above mentioned measures, the Meisterplan division also carries out the following measures for the Customer:

1. Access permissions to internal Meisterplan applications (JIRA, Stash, etc.) are regularly revised and reissued.

2. Only selected, long-standing, and specially trained and trusted employees of the Supplier have access to the Meisterplan AWS Production Infrastructure. A selection procedure is used to choose these employees.

3. Administrative access to the Meisterplan AWS infrastructure is logged.
4. Changes to how Meisterplan applications are deployed are logged via code versioning.

Access controls

1. Tool-assisted password management is utilized in all areas.
2. All in-house applications that are accessible through a browser over the Internet have TLS protected connections.
3. Protection against unauthorized access via the use of virus protection and firewall.

In addition to the above mentioned measures, the Meisterplan division also carries out the following measures for the Customer:

1. The user permissions of the employees depend on the respective area of responsibility of each employee. (They are issued according to the “need-to-know” principle).
2. SSO is offered for Meisterplan customers.
3. Meisterplan’s built-in authentication service ensures that Customer data can only be accessed by customers and not by others.

Transfer controls

1. Data is only transferred over an encrypted connection.
2. VPN access.

Input controls

1. Access to the system and data changes at the user level are logged in the central Customer Relationship Management System.

Transport controls

1. There is no transport of physical data storage media containing unencrypted third-party data neither within itdesign nor to subcontractors of itdesign.
2. Data storage media in notebooks is encrypted and secured with a password.

In addition to the above mentioned measures, the Meisterplan division also carries out the following measures for the Customer:

1. At Meisterplan no data storage media are sent to third parties or received from third parties. All data is exchanged using a file-sharing platform that utilizes an access rights and deletion concept and is accessible using a secure connection.
2. The use of USB sticks to process customer data is not allowed at Meisterplan.
3. All access to the Application data via http or SSH is encrypted.

Data recovery

1. Backup and recovery concept.
2. Backup operation control.
3. Utilization of a RAID system/disk mirroring.

In addition to the above mentioned measures, the Meisterplan division also carries out the following measures for the Customer:

1. Automated recovery of cloud computing resources in case of failure.

Reliability

1. Acoustic alarm in case of UPS/server malfunction.
2. Automatic notification in case of system failure.
3. Backup power supply of all production servers.
4. Annual training of employees on data protection guidelines.
5. All employees sign the declaration on data secrecy (§5 of the German Federal Data Protection Act (BDSG)). From 05/25/2018 onwards, employees obligate themselves to confidentiality based on Article 5 (1) et seq. and Article 32 (4) of the General Data Protection Regulation (GDPR).

In addition to the above mentioned measures, the Meisterplan division also carries out the following measures for the Customer:

1. High infrastructure redundancy (of computing, storage, and network resources) is provided through AWS. This ensures the very high availability of Meisterplan systems.
2. The system and infrastructure are monitored through the recording of various metrics, evaluation of logs, performance of health checks on the systems, and use of an alerting system.
3. An on-call technical support staff of 4 people (on rotation) is established and highly available.

4. The high quality of the application is ensured by conducting tests at all levels (unit tests, integration tests, e2e tests, UI tests, and manual tests with test plans). The company employs trained QA staff.
5. Incident management process with an improvement process.
6. Security is built into the Meisterplan development process. External verification is provided by a specialized pen test service provider.

Data integrity

1. Backup and recovery concept.
2. Backup operation control.
3. Monitoring of production systems.

Control of subprocessors

1. Cleaning service providers are carefully selected.
2. Employees who process the data of affected individuals are informed about the data processing agreements that have been concluded with the Client.
3. The employees that carry out processing of data under this Agreement are allowed to consult the data processing agreements, including the agreed technical organizational measures.
4. The approved technical organizational measures are monitored through recurring internal data protection audits.
5. Data processing agreements have been concluded with all subprocessors that are involved in processing of data under this Agreement.

Availability control

1. There is a fire extinguisher in the server room.
2. Devices for monitoring temperature and humidity have been installed in the server room.
3. The server room is climate controlled.
4. UPS system.
5. The entire building is equipped with fire and smoke detection systems.
6. Backups are kept in a secure, off-site location.
7. Utilization of a RAID system/disk mirroring.

In addition to the above mentioned measures, the Meisterplan division also carries out the following measures for the Customer:

1. The system and infrastructure are monitored through the recording of various metrics, evaluation of logs, performing health checks on the systems, and use of an alerting system.
2. An on-call technical support staff of 4 people (on rotation) is established and highly available.
3. Reporting on availability statistics is available.
4. For the security guidelines of the AWS Computing Center, see: https://aws.amazon.com/compliance/data-center/controls/

Separation of equipment

1. Test, development, and production systems are technically separated from each other.
2. Access authorizations to customer and employment data are controlled via user rights as well as via logical separation (labels in the data records) in the central Customer Relationship Management System.

Processing in compliance with instructions

In accordance with Art. 32 Para. 4 GDPR, it is to be ensured that employees and external service providers who have access to personal data process it only in accordance with the instructions of the person responsible. Therefore, the following measures are taken:

3. Obligation of employees to maintain data secrecy
4. Implementation of internal security guidelines
5. Training

Data Protection Management

The following additional procedures for regular review, assessment and evaluation shall be used pursuant to Art. 32, Para. 1(d) GDPR; Art. 25, Para. 1 GDPR:

6. Data protection management according to the PDCA Method
7. Incident response management
8. Data protection-friendly default settings pursuant to Art. 25, Para. 2 GDPR