Contract for the Processing of Personal Data on behalf of

Data Processing Agreement (DPA)

Between
gradwerk GmbH
Konrad-Adenauer-Straße 6
23558 Lübeck
Germany

hereinafter referred to as the "**Processor**" -

and

_____

_____

_____

_____

hereinafter referred to as the **Customer** -

both hereinafter referred to as "**the Parties**“
All terms are gender-neutral.

the following DPA is concluded:

Preamble and Scope of Application

The Processor is commissioned by the Customer to process personal data on behalf of the Customer. The DPA specifies this processing with regard to its object and the rights and obligations between the Contracting Parties arising from the Processing.
The DPA does not apply if the GDPR is not applicable to the processing of personal data by the Customer (for example, in the case of exclusively personal or family activities pursuant to Article 2 (2)(c) GDPR) and the Processor therefore does not act as a processor within the meaning of Article 4 (8) GDPR.

1. Terms and Definitions

a. "Processing" - Pursuant to 4 (8) GDPR, "Processing" is understood to mean the processing of personal data as defined in Article 4 (2) GDPR carried out on behalf of the Controller, irrespective of the number of intermediary processors, by the Processor in accordance with the subject-matter of this DPA.
b. "Principal Agreement" - The term " Principal Agreement" covers all types of ongoing business relations between the Customer and the Processor, under which the Processor processes personal data at the instruction of the Customer in accordance with the definition of the subject of the Processing in this DPA. Insofar as the validity of this DPA is otherwise limited (i.e. within this agreement or outside it, in other agreements or regulations) to certain types, categories or specific business relationships, contracts, etc., these are each to be understood as the Principal Agreement. The definition of the Principal Agreement also includes ongoing individual assignments by the Customer to the Processor, which are issued by the Customer within the scope of the Principal Agreement (e.g. in the case of framework contracts).
c. "Controller" - "Controller" is anyone who alone or jointly with others determines the purposes and means of processing (Article 4 (7) GDPR).
d. "Personal Data" - In accordance with Article 4 (1) GDPR, "personal data" (hereinafter also referred to briefly as "data") is all information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

e. "Data subjects" - In accordance with Article 4 (1) GDPR, "data subjects" are defined as Persons who are at least identifiable by means of personal data. The data subjects concerned by this Processing are determined by the subject-matter of the Processing.
f. "Third party" - "Third party" means according to Article 4 (10) GDPR a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
g. "Sub-processing" - When a processor is not directly appointed by the Controller but by a processor who is the first processor appointed by the Controller, a "sub-processing" is present and the processors following the first processor are referred to as "sub-processors".
h. "Electronic format" - declarations are deemed to have been made in "electronic format" in accordance with Article 28 (9) DSGVO if the declaring person is identifiable and the electronic declaration format is suitable as proof of the declaration. Electronic format" means in particular text form, an agreement stored on permanent data carriers (e.g. e-mail), digital signing procedures or the use of dedicated online functions (e.g. in user accounts).

2. Subject-Matter of the Processing

The detailed information on the subject-matter of the Processing, Data processed, the data subjects and the nature, scope and purposes of the Processing are governed by the provisions of the **Annex "The Subject-Matter of the Processing"**.

3. Type of Processing

Within the scope of this DPA, the Customer shall be responsible for compliance with the legal provisions of the data protection laws, in particular for the legality of the Processing and for the legality of the assignment of the processor.

4. Authority to issue instructions

a. The Processor may process Data only within the scope of the Principal Agreement and of the Customer's instructions and only insofar as Processing within the scope of the Principal Agreement is necessary.

b. The instructions are initially set out in the Principal Agreement or this DPA may subsequently be amended, supplemented or replaced by the Customer by issuing further instructions in writing or in an electronic format (text form, e.g. e-mail) to the Processor or to the entity designated by the Processor.
c. Oral instructions may be given if they are required by the circumstances (e.g. urgency) and must be confirmed immediately in writing or in electronical form.
d. If, on the basis of objective circumstances, the Processor considers that an instruction of the Customer is contrary to relevant data protection law, the Processor shall without delay inform the Customer thereof and provide objective reasons for his/her opinion. In this case, the Processor shall be entitled to suspend the execution of the instruction until the Customer expressly confirms the instruction and to refuse to execute the instruction in the case of obviously illegal instructions.
e. The Processor may be obliged to carry out processing operations or to communicate information by Union or Member State law and by administrative and judicial measures to which the Customer is subject. In such a case, the Processor shall communicate the legal requirements of the overriding legal obligation to the Customer prior to the processing, unless the law or order in question prohibits such communication on the grounds of an important public interest; in the event of a prohibition on communication, the Processor shall take possible and reasonable measures to prevent or restrict the legally overriding Processing.

5. Technical and Organisational Measures (Safety and Security Concept)

a. The Processor shall structure the internal organisation in his area of responsibility in accordance with the legal requirements and shall in particular implement technical and organisational measures (hereinafter referred to as "TOMs") for appropriate security, in particular the confidentiality, integrity and availability of the Customer's Data, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the Processing as well as the varying probability of occurrence and severity of the risk to the rights and freedoms of the persons concerned, and shall ensure that these measures are maintained, in particular by means of regular evaluation, at least once a year. With regard to the protection of the Data, the TOMs include in particular physical and logical access control, transfer control, input control, order control, integrity and availability control, separation control and the safeguarding of the rights of the Data Subjects.

b. The TOMs declared by the Processor upon conclusion of the contract define the minimum security level guaranteed by the Processor. The TOMs may and should be further developed in accordance with technical and legal progress and replaced by adequate protective measures, provided that they do not fall below the safety level of the defined measures and that any substantial changes are notified to the Customer. The description of the measures must be so detailed that a competent third party can at all times see beyond doubt that the required legal data protection level and the defined minimum security level are not undercut.

c. The Processor shall ensure that the employees, agents and other persons acting on behalf of the Processor are prohibited from processing the Data outside the scope of the Instruction. The Processor shall further ensure that the persons authorised to process the Client's Data have been instructed in the data protection provisions of law and of this DPA and have been bound to confidentiality and secrecy or are subject to a corresponding and appropriate legal obligation of secrecy. The Processor shall ensure that the persons employed for the Processing are with regard to the fulfilment of the data protection requirements appropriately instructed and supervised on an ongoing basis.

d. The Processor shall ensure that the persons employed by him/her to process the Data participate in a reasonable frequency of periodic training and awareness raising activities with regard to the protection of personal data and compliance with legal data protection requirements.

e. The processing of the Data outside of the premises of the Processor (e.g. in the home or mobile office or in case of remote access) is permitted, provided that the necessary technical and organisational measures are taken and documented, which take into account the specifics of these processing situations in an appropriate manner and in particular also allow sufficient control of the Data processing (e.g. conclusion of a data protection agreement with employees in the home and mobile office). The Processor shall provide the Principal with documentation of the implemented technical and organizational measures for such home, mobile or other remote processing upon request.

f. The Processing of personal data on the private devices of the employees of the Processor and its contractors is permitted, provided that the necessary technical and organisational measures are taken and documented, which take into account the specifics of these processing situations in an appropriate manner and, in particular, also allow for sufficient control of the Processing (e.g. conclusion of an agreement which allows for an appropriate control of the

private devices). On request, the Processor shall provide the Customer with documentation of the implemented technical and organisational measures for these types of Processing upon request.

g. If required by law, the processor shall appoint a data protection officer in accordance with the legal requirements. The Processor shall inform the Customer of the contact details of the data protection officer and of any subsequent changes.
h. The processing operations carried out for the Customer shall be separately recorded and documented by the Processor to an appropriate extent, and made available to the Customer on request.
i. The Data and data carriers and all copies made thereof, which are provided within the scope of the DPA, remain the property or ownership of the Customer, are subject to the Customer's control, must be carefully safeguarded by the Processor, protected from access by unauthorized third parties and may only be deleted, erased or disposed with the Customer's consent. Destruction must be carried out in accordance with data protection regulations and in such a way that a recovery of even residual information is no longer possible and cannot be expected with reasonable effort. Copies of data may only be made if they are necessary for the fulfilment of the principal and secondary obligations of the Processor towards the Customer (e.g. backups) and the contractual and statutory data protection level is guaranteed.
j. The processor shall be obliged to ensure the immediate return or deletion of the Data and data carriers, including those of sub-processors, in accordance with this DPA.
k. The right of retention is excluded with regard to the Data processed and the associated data carriers.
l. The Processor shall provide regular proof, to an appropriate extent, of the fulfilment of his/her obligations, in particular the full implementation of the agreed technical and organisational measures and their effectiveness (e.g. by regular checks, inspections, etc.). The proof is to be provided to the Customer upon request. The proof can be provided by approved rules of conduct or an approved certification procedure.
m. If the security measures taken do not or no longer meet the requirements of the Customer or the statutory requirements, the Processor shall notify the Customer immediately.
n. The technical and organizational measures already existing at the conclusion of this DPA are listed by the Processor in the **Annex "Technical and Organizational Measures"** and accepted by the Customer.

6. Information and cooperation obligations of the processor

a. The Processor may only provide information to third parties or the data subjects with the prior approval of the Customer. If a data subject contacts the Processor and asserts his or her rights as data subject (in particular rights of access or rectification or deletion of personal data), the Processor shall refer the data subject to the Customer, provided that, according to the data subject, an attribution to the Customer is possible. The Processor shall immediately forward the request of the data subject to the Customer and shall support the Customer within the scope of reasonableness and possibility. The Processor shall not be liable if the request of the data subject is not, not correctly or not timely answered by the principal, unless the Processor is responsible for this shortcoming.

b. The Processor shall immediately and fully inform the Customer if, with regard to the Processing, the Processor discovers errors or irregularities in the compliance with the requirements of this DPA and/or relevant data protection provisions. The Processor shall take the necessary measures to secure the Data and to mitigate any adverse consequences for the data subjects and shall consult with the Customer without delay.

c. The Processor shall inform the Customer without delay if a supervisory authority takes action against the Processor and whose activities may affect the Data processed for the Customer. The processor shall support the Customer in the fulfilment of his/her obligations (in particular to provide information and allow inspections) with regard to supervisory authorities.

d. Should the security of the Data be endangered (seizure, confiscation, insolvency proceedings, etc.) by measures taken by third parties (e.g. creditors, authorities, courts, etc.), the Processor shall inform the third parties without delay that the sovereignty and ownership of the Data lies exclusively with the Customer and, after consultation with the Customer, shall take appropriate protective measures (e.g. lodge objections, applications, etc.) if necessary.

e. The Processor shall provide the Customer with information relating to the Processing which is necessary for the fulfilment of the Customer's legal obligations (which may include, in particular, requests from data subjects or authorities and compliance with the Customer's accountability obligations of a data protection impact assessment).

f. The obligations of the Processor to provide certain information shall initially extend to information available to the Processor, his/her employees and agents. The information need not be obtained from third sources if the procurement by

the Customer could be carried out within reasonable limits and no other agreement has been made.

g. The Processor must at all times be able to demonstrate, by any appropriate means, compliance with his contractual and legal obligations resulting from the Processing.

7. Measures in the Event of a threat to Data Protection or Data Breach

a. In the event that the Processor becomes aware of facts which give rise to the assumption that the protection of the processed Data may have been breached within the meaning of Article 4 (12) GDPR, the Processor shall inform the Customer without delay and in full, take the necessary protective measures without delay, and assist the Customer in the performance of the Customer's obligations, in particular in relation to the notification of competent authorities or data subjects.
b. Information about a (possible) violation of the protection of the Data must be provided without undue delay, in general within 24 hours from the time of obtaining knowledge.
c. The notification from the Processor must according to Article 33 (3) GDPR contain at least the following information:
    a. description of the nature of the data breach or threat, specifying, where possible, the categories of data concerned and the approximate number of persons and personal data sets concerned;
    b. the name and contact details of the data protection officer or any other known contact point for further information;
    c. a description of the likely consequences of the data breach or threat (e.g. with further details: identity theft, financial loss, etc.);
    d. a description of the measures taken or proposed by the Processor to remedy the data breach and, where appropriate, measures to mitigate its possible adverse effects

8. Audits and Inspections

a. The Client has the right to control compliance with the legal requirements and the provisions of this DPA, in particular the TOMs at the Processor's premises at any time to the necessary extent, either himself or through third parties, and to carry out the necessary audits, including inspections.

b. The Processor shall support the Customer in the audits and inspections to the extent necessary (e.g. by providing personnel and granting access and access rights).
c. On-site inspections shall be carried out within normal business hours, shall be announced by the Customer within a reasonable period of time (at least 14 days). In emergencies, i.e. if waiting would endanger the rights of data subjects and/or the Customer to an unreasonable extent, an appropriately shorter period may be chosen. In the opposite case, a longer period may be necessary (e.g. if extensive preparations have to be made or during holiday periods). Deviations from the notice period must be justified by the Contracting Party requesting them.
d. The audits are limited to the necessary scope and must take into account the business and trade secrets of the Processor and the protection of personal data of third parties (e.g. other customers or employees of the Processor). Any interruptions to operations that are preventable must be avoided. Insofar as sufficient for the reason and purpose of the audit, an audit shall be limited to spot checks.
e. Only qualified personnel who are able to prove their identity and who are obliged to maintain confidentiality and secrecy with regard to the company and business secrets, other personal data and internal processes of the Processor are permitted to carry out the audit. The Processor may request proof of an appropriate commitment of the auditors. If the auditor appointed by the Customer is in a competitive relationship with the Processor or if there is any other justified reason for his/her refusal, the Processor shall have the right to object the appointment of the auditor.
f. Instead of audits and on-site inspections, the Processor may refer the Customer to an equivalent audit by independent third parties (e.g. neutral data protection auditors), compliance with approved rules of conduct (Article 40 GDPR) or appropriate data protection or IT security certifications pursuant to Article 42 GDPR. This shall only apply if the reference is reasonable for the client and the nature and scope of the audit and references correspond to the nature and scope of the client's legitimate audit and inspection intentions. The Processor shall immediately notify the Client of the exclusion of approved rules of conduct pursuant to Article 41(4) GDPR, the revocation of a certification pursuant to Article 42(7) GDPR and any other form of revocation or substantial modification of the above-mentioned proofs.
g. As a rule, the client does not exercise his right of audit more frequently than every 12 months, unless a specific reason (in particular a violation of data

protection, a security incident or the result of an other audit) makes it necessary to carry out audits before the end of this period.

9. Sub-Processing

a. Sub-processors may be assigned by the Processor only with a prior specific written (including in electronic form) authorisation of the Customer. Such authorisation may not be withheld on undue or unreasonable grounds.
b. Without prejudice to any restrictions imposed by the Principal Agreement, the Customer expressly agrees that the Processor may use sub-processors in the context of the Processing. The Processor shall inform the Customer of any new sub-processors within a reasonable period of time, which shall normally be 14 working days, and shall give the Customer the opportunity to reasonably inspect the sub-processors before using them and to object to the use of sub-processors if the Customer has a legitimate interest. If the Customer does not raise an objection within the preliminary period, the authorisation shall be deemed to have been granted. The Customer shall exercise the right to object to the changes only in accordance with the principles of good faith and of reasonableness and fairness.
c. If the processor uses the services of a sub-processor (e.g. a subcontractor) in order to carry out certain Processing activities on behalf of the Customer, it must impose on the sub-processor, by means of a contract or any other legal instrument permitted by law, the same data protection obligations as those to which the Processor has committed him/herself in this DPA (in particular as regards following instructions, complying with the TOMs, providing information and allowing audits).
d. The sub-processor shall be carefully selected by the Processor, having particular regard to the suitability and reliability of the sub-processor to comply with the obligations under this DPA for Processing and the adequacy of the TOMs implemented by the sub-processor.
e. The Processor shall be required to document the verification of the reliability of sub-processors and the legality of their assignment and to submit it to the Customer on request.
f. The Processor shall audit compliance with the obligations of the sub-processors, in particular the TOMs, on a regular basis and at least every 12 months, to an appropriate extent. The inspection and its results shall be documented in a comprehensible manner so that they are comprehensible to a competent third party. The documentation shall be presented to the Customer on request.

Instead of his own audit, the Customer may refer to an audit by independent third parties (e.g. neutral data protection auditors), compliance with approved rules of conduct (Article 40 GDPR) or suitable data protection or IT security certifications in accordance with Article 42 GDPR. The Customer shall immediately notify the Customer of the exclusion of approved rules of conduct pursuant to Art. 41 (4) GDPR, the revocation of a certification pursuant to Art. 42 (7) GDPR and any other form of revocation or substantial modification of the above-mentioned proofs.

g. The responsibilities for performing the obligations under this DPA and under the law must be clearly defined and allocated between the processor and the sub-processor.
h. The Processor shall be liable to the Customer in the event that the sub-processor fails to comply with his/her data protection duties.
i. Processing of personal data which is not directly related to the provision of the main contractual obligation and where the Processor uses the assistance of third parties as a mere ancillary service in order to carry out its business activity (e.g. cleaning, security, maintenance, telecommunications or transport services) does not constitute sub-processing within the meaning of the above provisions of this DPA. Nevertheless, the processor shall ensure, e.g. by contractual agreements or notices and instructions, that the security of the data is not endangered and that the provisions of this processing contract and the data protection regulations are observed.
j. Sub-processing relationships of which the Customer was notified at the time of the conclusion of this DPA shall be deemed approved to the extent of the notification and subject to the provisions of this DPA on sub-processing.
k. The sub-processing relationships already in existence at the time of the conclusion of this DPA are listed by the Processor in the Annex "Sub-Processors" and updated by the Processor.

10. Spatial Area of the Processing

a. The Data is processed within the scope of the DPA in a member state of the European Union (EU) or in another member state of the Agreement on the European Economic Area (EEA) or in Switzerland.
b. Processing may take place in third countries provided that the special conditions laid down in Article 44 et seq. GDPR are fulfilled, i.e. in particular a) the EU Commission has established an adequate level of data protection; or b) on the basis of so-called Standard Contractual Clauses (SCC); or c) on the basis of binding corporate rules.

c. The authorisation of sub-contractingessing relationships by the Customer within the scope of this DPA, shall also extend to the spatial area of the Processing.
d. Processing in a country other than those referred to in the preceding paragraphs, including by sub-processors, shall be subject to the prior consent of the Customer.

11. Obligations of the Customer

a. The Customer must inform the Processor without delay and in full if he/she discovers errors or irregularities in the Processing results, instructions or processing procedures with regard to data protection regulations.
b. In the event of a claim against the Processor by data subjects, third parties, bodies or authorities with regard to possible entitlements arising from the processing of the Data within the scope of this DPA, the Customer undertakes to support the Processor in the defence of the claim within the scope of its possibilities and taking into account the degree of fault of the Contracting Parties.

12. Liability

The statutory liability provisions apply, in particular Article 82 GDPR and, in the case of the use of a sub-processor, Article 28 (4) S. 2 GDPR.

13. Term, Continuation after Termination of the DPA and Deletion of Data

a. This DPA becomes effective upon its signature or conclusion in an electronic format.
b. The effective term and termination of this DPA shall be determined by the erm and termination of the Principal Agreement.
c. The DPA may be terminated by either Contractual Party by giving three months' notice.
d. The right of extraordinary termination is reserved to the Contractual Parties, in particular in the event of a serious breach of the obligations and specifications of this DPA and the applicable data protection law. A serious breach shall be deemed to have occurred in particular if the Processor fails or has failed to perform to a considerable extent the duties specified in the DPA and the agreed technical and organisational measures.

e. In the case of non-material breaches of duty, the termination for good cause must be preceded by a warning notice of the breaches with a reasonable period of notice to remedy them, whereby the warning notice is not required if it is not to be expected that the breaches complained of will be remedied or if they are so substantial that the terminating Contractual Party cannot reasonably be expected to adhere to the DPA.
f. The termination of the Agreement, as well as the termination of this clause must be made at least in electronic format.
g. Upon completion of the Processing under this DPA, the Processor shall, at the Customer's discretion, either destroy or return all Data and copies thereof (as well as all documents, processing and usage results and data files coming into its possession in connection with the contractual relationship), unless there is a legal obligation to store the Data, in which case the Processor shall inform the Customer of the obligation and its scope, unless the Customer can be expected to be aware of the obligation. The destruction or deletion must be carried out in accordance with data protection regulations and in such a way that a recovery of even residual information is no longer possible or cannot be expected with reasonable effort. The objection of a right of retention is excluded with regard to the processed Data and the associated data carriers. With regard to the deletion or return, the rights of the Customer to information, proof and audit apply in accordance with this DPA.
h. The obligations to protect confidential information arising from the DPA shall continue to apply after the end of the DPA, provided that the Processor continues to process the Personal Data covered by the DPA and that compliance with the obligations can reasonably be expected of the Processor even after the end of the DPA.
i. Documentation which serves as proof of proper data processing and safeguarding of the TOMs shall be kept by the Processor in accordance with the Customer's respective retention and deletion periods, at least three years also beyond the end of the contract. The Processor may hand over the documentation to the Customer at the end of the contract in order to discharge the Processor from the duty to archive documents.

14. Reimbursement of expenses

a. Additional expenses incurred in supporting the Customer in the fulfilment of its obligations under data protection law or other obligations shall be appropriately remunerated at the hourly rates specified in the Principal Agreement.

b. The reimbursement of expenses or remuneration agreed under the DPA shall also include an allowance for the working hours of the personnel used by the Processor as well as necessary expenses (e.g. travel or material costs). To the extent possible, foreseeable and reasonable, the Processor shall notify the Customer of the amount of the reimbursement or remuneration by way of a proper estimate before it is incurred.
c. If the expenditure for the Processor with the Customer's instructions exceeds the scope agreed upon in the Principal Agreement or otherwise expected to be customary in the industry, and the Processor is not at fault, the Customer shall compensate the Processor separately for the additional expenditure incurred.
d. If the expenditure for the Processor in connection with the provision of information and/or the necessary cooperation of the Processor exceeds the scope agreed upon in the Principal Agreement or otherwise expected to be customary in the industry, and the Processor is not at fault, the Customer shall compensate the Processor separately for the additional expenditure incurred.
e. If the expenditure for the Processor with participation in the audits or adequate alternative measures exceeds the scope agreed upon in the Principal Agreement or otherwise expected to be customary in the industry, and the Processor is not at fault, the Customer shall compensate the Processor separately for the additional expenditure incurred.
f. If the expenditure for the Processor with the deletion or the return of the data exceeds the scope agreed upon in the Principal Agreement or otherwise expected to be customary in the industry, and the Processor is not at fault, the Customer shall compensate the Processor separately for the additional expenditure incurred.

15. Final Provisions

a. The applicable law is determined by the statutory provisions.
b. The exclusive place of jurisdiction for all disputes arising out of or in connection with this DPA shall be the residential domicile or the (registered) office of the Processor and insofar as mandatory by applicable law, the Customer is a merchant, a legal entity under public law or a special fund under public law or if the the Customer has no place of jurisdiction within the jurisdiction of the applicable law. The Processor reserves the right to assert claims at the statutory place of jurisdiction.
c. The DPA constitutes the entire agreement concluded between the Contractual Parties. There are no additional agreements.

d. With the conclusion of this DPA, all previous contracts, if any, concluded between the parties to this contract and which regulate the Processing of the Data on behalf of the Customer are revoked, if and insofar as they relate to the same subject-matter of this DPA and if and insofar as the parties have not expressly agreed otherwise in writing.
e. Amendments and additions to this DPA, as well as the termination of this clause must be made at least in electronic format.
f. In the event of a conflict with the Principal Agreement, the DPA shall take precedence.
g. Should one or more provisions of this DPA be invalid or unenforceable, this shall not affect the validity of the remaining provisions. Rather, the invalid provisions shall be replaced by way of a supplementary interpretation by such a provision which comes as close as possible to the economic purpose visibly pursued by the parties with the invalid provision(s). If the above-mentioned supplementary interpretation is not possible due to legally binding requirements, the Contracting Parties shall agree on a corresponding provision.

.....

Place, date, signature Controller

.....

Place, date, signature Processor

16. Annex: Subject-Matter of the Processing

Purposes of Processing

Personal data of the Customer shall be processed on the basis of this Data Processing Agreement for the following purposes:

a. Consulting services
b. Support and administration of websites, social media and other communication and information channels.
c. Creation and/or processing of personal profiles
d. Email marketing.
e. Installation, maintenance and support of information technology equipment and systems (IT).
f. Collection and processing of contact information, addresses and leads.
g. Customer management and / or customer support.
h. Software-as-a-Service (SaaS).
i. Services in the field of software development and / or maintenance.
j. Corporate communication (internal/external).
k. Administrative, management and / or governance services.
l. Web and Cloud Hosting
m. (consulting, conception, implementation and realisation).

Types and Categories of Data

The types and categories of personal data processed on the basis of this DPA include:

a. Master/ Inventory data.
b. Contact information.
c. Content data.
d. Images and/or video recordings.
e. Contract details.
f. Payment data and billing data.
g. Creditworthiness data.
h. Usage data.
i. Location data.
j. Data of lottery participants.
k. Log data.
l. Meta/communication data.
m. Employee data.
n. Salary data.
o. Performance and behaviour data.
p. Applicant data

q. Business Information.
r. Member data.

Processing of Special Categories of Data

The special categories of personal data processed on the basis of this DPA (pursuant to Art. 9 (1) GDPR) include:

a. Daten aus denen die rassische Herkunft hervorgeht.
b. Data revealing ethnic origin.
c. Data revealing religious or philosophical beliefs.
d. Data revealing trade union membership.

Sources of the Processed Data

The categories of data subjects affected by the processing of personal data on the basis of this DPA include:

a. Website visitors.
b. Software users.
c. Target groups of marketing measures.
d. Participants.
e. Subscribers.
f. Prospective customers.
g. Consumers.
h. Business customers.
i. Business partners.
j. Freelancers.
k. Employees / workers.
l. Applicants.
m. Students
n. Members

Sources of the Processed Data

The data processed on the basis of this DPA are collected or otherwise received from the sources or within the framework of the procedures mentioned below:

a. Collection from data subjects.
b. Inputs or information provided by the Customer.
c. Inputs or information provided by the Processor.
d. Collection in the context of the use of software, websites and other online services.
e. Collection in connection with events and meetings.
f. Collection in connection with advertising and marketing campaigns.
g. Collection via interfaces to services of other providers.
h. Externe Datenbanken und Datensammlungen

i. Reception by means of transmission or other communication by or on behalf of the Customer.

Appendix: Competent Persons and Contact Persons

The contact persons named below are authorized to issue or receive instructions from the Customer.Changes in contact persons, their non-temporary disability or their contact details must be notified to the other Party.

Annex: Technical and Organisational Measures (TOMs)

An adequate level of protection is ensured for the Processing and the Data processed, which is appropriate to the risks for the interests or fundamental rights and freedoms of data subjects concerned. To this end, especially the protection objectives of confidentiality, integrity and availability of the systems and services and their resilience with respect to the nature, extent, circumstances and purposes of the Processing shall be taken into account in such a way that the risk is mitigated on a lasting basis by appropriate technical and organisational remedial measures.

Data Protection at Employee Level

Measures have been taken to ensure that employees involved in the processing of personal data have the necessary expertise and reliability required by data protection law.

a. Employees are bound to confidentiality and secrecy with regard to data protection.
b. Employees are made aware of and informed about data protection in accordance with the requirements of their function. The training and awareness raising is repeated at appropriate intervals or as and when required by circumstances.
c. The keys, access cards or codes issued to employees, as well as authorisations granted with regard to the processing of the Data, shall be collected or revoked after they leave the services of the Processor or after the change of their responsibilities.

Physical Access Control

Physical access control measures have been taken to prevent unauthorised persons from physically approaching the systems, data processing equipment or procedures by which the Data are processed.

a. Access to data processing systems is especially secured and only authorised employees can physically access them.
b. An alarm system is used to prevent access by unauthorised persons.
c. The access is secured by a manual locking system with security locks.
d. The issue and return of keys and/or access cards is logged.
e. Employees are required to lock or specially secure equipment when they leave their work environment or the equipment.

f. Records (files, documents, etc.) will be stored in a secure manner, e.g. in filing cabinets or other adequately secured containers and adequately protected against physical access by authorised persons.
g. Data carriers are stored securely and adequately protected against access by unauthorised persons.

Electronic Access Control

Electronic access control measures have been put in place to ensure that access (i.e. already the possibility of exploitation, use or observation) by unauthorised persons to systems, data processing equipment or procedures is being prevented.

a. A password concept specifies that passwords must have a minimum length and complexity in line with the state of the art and security requirements.
b. All data processing systems are password protected.
c. Passwords are generally not stored in plain text and are only transmitted hashed or encrypted.
d. A password management software is used.
e. Failure to login to internal systems will be limited to an appropriate number (e. g. by disabling of login credentials).
f. Access credentials are deleted or deactivated when their users have left the company or organization of the Processor.
g. Up-to-date anti-virus software is used.
h. Use of software firewall(s).
i. Backups are stored in encrypted form.

Internal Access Control (permissions for user rights of access to and amendment of data)

Internal access control measures have been put in place to ensure that persons authorised to use a data processing system can only access the Data covered by their access authorisation and that personal data cannot be read, copied, modified or removed without authorisation during the Processing. Furthermore, input control measures have been taken to ensure that it is possible to subsequently check and establish whether and by whom the Data have been input, modified, removed or otherwise processed in data processing systems.

a. A rights and roles concept (authorisation concept) ensures that access to personal data is only possible for a group of people selected according to necessity and only to the extent necessary.
b. The rights and roles concept (authorisation concept) is evaluated regularly, within a reasonable time frequency and when required by an occasion (e.g. violations of access restrictions), and updated as necessary.
c. The activities of the administrators are appropriately monitored and recorded to the extent permitted by law and to the extent technically feasible.

Transmission Control

Measures have been taken to control the transmission of the Data to ensure that the Data cannot be read, copied, modified or deleted by unauthorised persons during electronic transmission or during their transport or storage on data carriers, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

a. When accessing internal systems from outside (e.g. for remote maintenance), encrypted transmission technologies are used (e.g. VPN).
b. The transmission and processing of the client's personal data via online offers (websites, apps, etc.) is protected by TLS/SSL or equivalent secure encryption.

Adherence to Instructions, Purpose Limitation and Separation Control

Measures have been taken to ensure that Data processed on behalf of the Customer are only processed in accordance with the instructions of the Customer. The measures ensure that the Data collected for different purposes are processed separately and that there is no merging, combining or other combined processing of the Data contrary to the instructions.

a. Careful selection of sub-processors and other service providers.
b. Employees and agents are informed in a clear and comprehensible manner about the instructions of the Customer and the permitted processing framework and are trained accordingly. Separate information and training is not required if compliance with the instructions can be reasonably expected in any event, e.g. due to other agreements or internal practice.
c. Compliance with instructions of the Customer and the permissible scope of processing of personal data by employees and contractors of the Processor is reviewed at appropriate intervals.

d. The Data of the Customer shall be processed logically separated from data of other processing operations of the Processor and protected against unauthorised access or connection or combination or mixing with other data (e.g. by storage in different databases or by appropriate attributes).

Safeguarding the Integrity and Availability of Data and the Resilience of Processing Systems

Measures have been taken to ensure that personal data are protected against accidental destruction or loss and can be quickly restored in an emergency.

a. Fail-safe server systems and services are used, which are designed as redundant dual or multiple systems.
b. The Data is stored with external hosting providers. The hosting providers are carefully selected and comply with the state of the art in terms of protection against damage caused by fire, moisture, power failures, disasters, unauthorized access, data backup and patch management as well as facility security.
c. The Processing of Data is carried out on data processing systems which are subject to regular and documented patch management, i.e. in particular regularly updated.
d. The server systems used for processing have protection against Denial of Service (DoS) attacks.
e. The server systems used for processing have an uninterruptible power supply (UPS), which is adequately secured against failures and ensures a controlled shutdown in emergencies without data loss.
f. Intrusion (physical) and contact detectors at the server location.
g. The server systems used for processing have adequate fire protection (fire and smoke detection systems and appropriate fire extinguishing devices or fire extinguishing equipment).
h. Server systems are used that have protection against moisture damage (e.g. moisture detectors).
i. The Customer's data records are protected by the system against inadvertent modification or deletion (e.g. by access restrictions, security checks and backups).
j. Server systems and services are used which have an appropriate, reliable and controlled backup & recovery concept.

Annex: Sub-Processors

The Processor shall use the following sub-processors in the Processing of data on behalf of the Client:

- **Timme Hosting GmbH & Co. KG:** Services in the field of provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Order processing agreement:** provided by the provider for customers; **Service provider:** Timme Hosting GmbH & Co. KG, Ovelgönner Weg 43, 21335 Lüneburg, Germany; **Website:** https://timmehosting.de; **Privacy policy:** https://timmehosting.de/datenschutz.
- **DomainFactory:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider**: domainfactory GmbH, Oskar-Messter-Str. 33, 85737 Ismaning, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.df.eu; **Privacy Policy:** https://www.df.eu/de/datenschutz; **Data Processing Agreement:** https://www.df.eu/de/support/formulare/.
- **HostEurope:** Services in the field of the provision of information technology infrastructure and related services (e.g. storage space and/or computing capacities); **Service provider**: Host Europe GmbH, Hansestrasse 111, 51149 Cologne, Germany; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://www.hosteurope.de/en; **Privacy Policy:** https://www.hosteurope.de/en/terms-and-conditions/privacy; **Data Processing Agreement:** https://www.hosteurope.de/Dokumente/.
- **Synology C2:** Backup service and backup server; **Service provider:** Synology GmbH, Grafenberger Allee 295, 40237 Düsseldorf, Germany; **Legal basis:** Legitimate interests (Art. 6 para. 1 p. 1 lit. f. DSGVO); **Website:** https://c2.synology.com/de-de/backup/business/overview; **Privacy policy:** https://www.synology.com/de-de/company/legal/privacy

Annex: Optional sub-processors

The Processor shall use the following sub-processors only on a case-by-case basis and after separate instruction by the Client in the context of the processing of data for the Client, the sub-processors used accordingly shall be **ticked** below.

- ☐ **Google Fonts (Provision on own server):** Obtaining fonts ("Google Fonts") for the purpose of a user-friendly appearance of our online services; **Service provider**: The Google Fonts are hosted on our server, no data is transmitted to Google; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR).
- ☐ **MyFonts and Fonts.com:** fonts; data processed in the font request process includes the identification number of the web font project (anonymized), the URL of the licensed website associated with our number to identify the licensee and the licensed web fonts, and the referrer URL; the anonymized web font project identification number is stored in encrypted log files with such data for 30 days to determine the monthly number of page views; after such extraction and storage of the number of page views the log files are deleted; Legal Basis: Legitimate Interests (Article 6 (1) (f) GDPR); **Service provider**: Monotype Imaging Holdings Inc., 600 Unicorn Park Drive, Woburn, Massachusetts 01801, USA; **Website:** https://www.myfonts.co; **Privacy Policy:** https://www.myfonts.com/info/legal/#Privacy.
- ☐ **Mapbox:** Provision and editing of geographic and other maps, plans, and location-based information; **Service provider**: https://www.mapbox.com/; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Legal Basis:** Mapbox, Inc., 740 15th St Nw Suite 500 Washington, DC 20005 USA; **Privacy Policy:** https://www.mapbox.com/legal/privacy; **Data Processing Agreement:** Provided by the service provider; **Standard Contractual Clauses (Safeguarding the level of data protection when processing data in third countries):** see Data Processing Agreement.

- ☐ **Google Maps:** We integrate the maps of the service "Google Maps" from the provider Google. The data processed may include, in particular, IP addresses and location data of users, which are not collected without their consent (usually within the framework of the settings of their mobile devices); **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://cloud.google.com/maps-platform; **Privacy Policy:** https://policies.google.com/privacy; **Opt-Out:** Opt-Out-Plugin: https://tools.google.com/dlpage/gaoptout?hl=en, Settings for the Display of Advertisements: https://adssettings.google.com/authenticated.
- ☐ **Google Maps APIs and SDKs:** Interfaces to the map and location services provided by Google, which, for example, allow the addition of address entries, location determinations, distance calculations or the provision of supplementary information on locations and other places; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; **Legal Basis:** Legitimate Interests (Article 6 (1) (f) GDPR); **Website:** https://cloud.google.com/maps-platform; **Privacy Policy:** https://policies.google.com/privacy.
- ☐ **Instagram Ads:** Placement of ads within the Instagram platform and analysis of ad results; **Service provider**: Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://www.instagram.com; **Privacy Policy:** https://instagram.com/about/legal/privacy; **Opt-Out:** We refer to the data protection and advertising settings in the user's profile on the Instagram platform as well as Instagram's consent procedure and Instagram's contact options for exercising information and other data subject rights in Instagram's privacy policy; **Further Information:** User event data, i.e. behavioral and interest data, is processed for the purposes of targeted advertising and audience building on the basis of the joint controllership agreement ("Controller Addendum", https://www.facebook.com/legal/controller_addendum). The joint controllership is limited to the collection and transfer of the data to Meta Platforms Ireland Limited, a company located in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which concerns in particular the transfer of the data to the parent company Meta Platforms, Inc. in the USA (on the basis of standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).

- ☐ **Facebook Ads:** Placement of ads within the Facebook platform and analysis of ad results; **Service provider**: Meta Platforms Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://www.facebook.com; **Privacy Policy:** https://www.facebook.com/about/privacy; **Opt-Out:** Wir verweisen auf die Datenschutz- und Werbeeinstellungen im Profil des Nutzers auf der Facebook-Plattform sowie auf das Einwilligungsverfahren von Facebook und die Kontaktmöglichkeiten von Facebook zur Ausübung von Informations- und sonstigen Betroffenenrechten in der Datenschutzerklärung von Facebook; **Further Information:** User event data, i.e. behavioral and interest data, is processed for the purposes of targeted advertising and audience building on the basis of the joint controllership agreement ("Controller Addendum", https://www.facebook.com/legal/controller_addendum). The joint controllership is limited to the collection and transfer of the data to Meta Platforms Ireland Limited, a company located in the EU. Further processing of the data is the sole responsibility of Meta Platforms Ireland Limited, which concerns in particular the transfer of the data to the parent company Meta Platforms, Inc. in the USA (on the basis of standard contractual clauses concluded between Meta Platforms Ireland Limited and Meta Platforms, Inc.).
- ☐ **Google Ads and Conversion Tracking:** We use the Google "Ads" online marketing method to place ads on the Google advertising network (e.g., in search results, videos, websites, etc.) so that they are displayed to users who have an alleged interest in the ads. We also measure the conversion of the ads (so called "Konversion"). However, we only know the anonymous total number of users who clicked on our ad and were redirected to a page tagged with a conversion tracking tag. However, we ourselves do not receive any information that can be used to identify users; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://marketingplatform.google.com; **Privacy Policy:** https://policies.google.com/privacy; **Further Information:** Types of processing and data processed: https://privacy.google.com/businesses/adsservices; Google Ads Controller-Controller Data Protection Terms and standard contractual clauses for data transfers to third countries: https://business.safety.google/adscontrollerterms.
- ☐ **Google Tag Manager:** Google Tag Manager is a solution with which we can manage so-called website tags via an interface and thus integrate other services into our online services (please refer to further details in this privacy policy). With

the Tag Manager itself (which implements the tags), for example, no user profiles are created or cookies are stored. Google only receives the IP address of the user, which is necessary to run the Google Tag Manager; **Service provider**: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, parent company: Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; **Legal Basis:** Consent (Article 6 (1) (a) GDPR); **Website:** https://marketingplatform.google.com; **Privacy Policy:** https://policies.google.com/privacy; **Data Processing Agreement:** https://business.safety.google/adsprocessorterms; **Standard Contractual Clauses (Safeguarding the level of data protection when processing data in third countries):** https://business.safety.google/adsprocessorterms; **Further Information:** https://privacy.google.com/businesses/adsservices (Types of processing and data processed).

Status: 28 November 2022