

**Agreement on the Processing on Behalf of a Controller according to
Art. 28 para. 3 – General Data Protection Regulation
(REGULATION (EU) 2016/679)**

BETWEEN

[name of clinic]

[name of practitioner]

[clinic address]

[country]

in the following ***Customer***

AND

Modern Me GmbH

Benrather Schlossallee 31

40597 Düsseldorf

Germany

in the following ***Contractor***

1 Introduction, Scope, Definitions

- (1) This Agreement regulates the rights and obligations of the Customer and Contractor (hereinafter referred to as "Parties") in the context of the processing of personal data on behalf of the Customer.
- (2) This Agreement applies to all activities in which employees of the Contractor or subcontractors commissioned [ordered] by the Contractor process personal data of the Customer on its behalf.
- (3) Terms used in this Agreement shall be understood under their definition in the EU GDPR. In this sense, the Customer is the "controller", the Contractor is the "processor".

2 Subject Matter and Duration of the Processing

2.1 Subject Matter

The Contractor shall undertake the following processing operations: Analyzing digital dental scans, clinical photos, treatment plans, creating 3D simulations, the preparation of estimates and invoices, services, consulting and the production of dental aligners.

2.2 Duration

Processing shall begin on [date] and continue indefinitely until termination of this Agreement.

3 Nature, Purpose and Data Subjects of the Data Processing:

3.1 Nature and Purpose of the Processing

The nature of the processing is as follows: collection, recording, organization, filing, storage, adaptation or alteration, reading, retrieval, use, disclosure by transmission, dissemination or otherwise making available, cross-checking or linking, limitation, erasure or destruction of data

The purpose of the processing is as follows: processing of orders from companies / dentist / orthodontists / clients for their customers / patients for consultation, preparation of cost estimates and 3D simulations, production of dental aligners, dental retainers, as well as invoicing, operation of the website, the web portal for companies / dentist / orthodontists / clients as well as electronic contract conclusion for order processing via service providers.

3.2 Type of Data

The following data is processed:

- Any data required to fulfill the above-described purpose and contractual obligations. The specific data processed may consist of first name, last name/surname, maiden name, date of birth, gender, clinical photos, x-ray images, health data.

3.3 Categories of Data Subjects

The following are data subjects of the processing:

- Natural persons who are a patient of the Customer (Customer = dentist / orthodontists / companies from the dental industry)

4 Duties of the Contractor

- (1) The Contractor shall process personal data only as contractually agreed or as instructed by the Customer, unless the Contractor is obliged by law to carry out a specific processing. If such obligations exist for the Contractor, it shall notify the Customer thereof prior to processing, unless such

notification is prohibited by law. Furthermore, the Contractor shall not use the data provided for processing for any other purpose, in particular not for its own purposes.

- (2) The Contractor confirms that it is aware of the relevant, general data protection regulations. It observes the principles of proper data processing.
- (3) The Contractor undertakes to maintain strict confidentiality during processing.
- (4) Persons who may gain knowledge of the data processed in the commissioning must agree in writing to maintain confidentiality, unless they are already legally subject to a relevant confidentiality obligation.
- (5) The Contractor warrants that the persons employed by it for processing have been made familiar with the relevant provisions of data protection and this Agreement prior to commencement of processing. Appropriate training and awareness-raising measures shall be appropriately repeated on a regular basis. The Contractor shall ensure that persons employed for commissioned data processing are instructed and monitored appropriately on an ongoing basis with regard to the fulfilment of data protection requirements.
- (6) In connection with the commissioned processing, the Contractor shall support the Customer to the extent necessary in fulfilling its data protection obligations, in particular in compiling and updating the list of processing activities, in carrying out the data protection impact assessment and a necessary consultation with the supervisory authority. The necessary information and documentation shall be kept available and shall be forwarded without delay to the Customer upon request.
- (7) If the Customer is subject to inspection by supervisory authorities or other bodies, or if data subjects assert rights against it, the Contractor undertakes to support the Customer to the extent necessary insofar as the commissioned processing is concerned.
- (8) The Contractor may provide information to third parties or the data subjects only with the prior consent of the Customer. It shall immediately forward requests addressed directly to it to the Customer.
- (9) Insofar as required by law, the Contractor shall appoint a competent and reliable person as data protection officer (DPO). It shall be ensured that the DPO has no conflicts of interest. In cases of doubt, the Customer can contact the DPO directly. The Contractor shall inform the Customer immediately of the contact details of the DPO or give a reason why no DPO has been appointed. The Contractor shall inform the Customer immediately of any changes in the identity or internal tasks of the DPO.
- (10) The commissioned data processing generally takes place within the EU or EEA. Any transfer to a third country may take place only with the express consent of the Customer and subject to the conditions in Chapter V of the GDPR and in compliance with the provisions of this Agreement.
- (11) If the Contractor is not established in the European Union, it shall appoint a responsible contact person in the European Union under Art. 27 of the GDPR. The contact data of the contact person as well as all changes in the identity of the contact person are to be communicated to the Customer immediately.

5 Security of Processing

- (1) The data security measures described in Attachment 1 are made mandatory. They define the minimum owed by the Contractor. The description of the measures must be so sufficiently detailed as to enable a competent third party to know beyond doubt at any time, on the basis of the description alone, what the required minimum amount should be. A reference to information which cannot be directly taken from this Agreement or its attachments is impermissible.
- (2) The data security measures can be adapted to the technical progress and further organizational development as long as the level does not fall below the level agreed to here. The Contractor shall immediately implement any changes required to maintain information security. The Customer must be informed immediately of any changes. Material changes must be agreed to between the parties.
- (3) If the security measures taken do not or no longer meet the Customer's requirements, the Contractor shall notify the Customer immediately.

- (4) The Contractor warrants that the commissioned data processed will be strictly separated from other data files.
- (5) Copies or duplicates will not be made without the knowledge of the Customer. Technically necessary, temporary duplications are excluded, as far as an impairment of the data protection level agreed to here is excluded.
- (6) The processing of data in private homes is permitted. Insofar as such processing takes place, the Contractor shall ensure that a level of data protection and data security corresponding to this Agreement is maintained and that the control rights of the Customer specified in this Agreement can be exercised without restriction also in the private homes concerned. The commissioned data processing with private devices is not permitted under any circumstances.
- (7) Dedicated data carriers that originate at the Customer or are used for the Customer are specially marked and subject to ongoing administration. They must be stored appropriately at all times and must not be accessible to unauthorized persons. Incoming and outgoing data carriers are documented.
- (8) The Contractor shall provide regular verification of the fulfilment of its obligations, in particular the complete implementation of the agreed technical and organizational measures and their effectiveness. The verification shall be provided to the Customer at the latest every 12 months without being requested to do so and otherwise at any time upon request. This can be demonstrated by approved codes of conduct or an approved certification procedure. Verification shall be kept for at least three calendar years after completion of commissioned data processing and shall be submitted to the Customer at any time upon request.

6 Regulations for the Rectification, Deletion and Blocking of Data

- (1) The Contractor shall rectify, delete or block data processed within the scope of this Agreement only under the contractual agreement or instructions of the Customer.
- (2) The Contractor shall follow the corresponding instructions of the Customer at all times and also beyond the termination of this Agreement.

7 Subcontracting Relationships

- (1) The commissioning of subcontractors is permitted only with the written consent of the Customer in individual cases.
- (2) Such consent shall be possible only if the subcontractor has at least been contractually obliged to comply with data protection obligations at least comparable to those agreed to in this Agreement. Upon request, the Customer shall have access to the relevant contracts between Contractor and subcontractor.
- (3) It must also be possible for the Customer to effectively exercise its rights towards the subcontractor. In particular, the Customer must be entitled to carry out inspections at any time to the extent specified here, also at subcontractors, or to have them carried out by third parties.
- (4) The responsibilities of the Contractor and subcontractor shall be clearly distinguished.
- (5) Further subcontracting by the subcontractor is not permitted.
- (6) The Contractor shall carefully select the subcontractor, particularly considering the suitability of the technical and organizational measures taken by the subcontractor.
- (7) The forwarding of data commissioned to be processed to the subcontractor is allowed only if the Contractor has been convinced in a documented form that the subcontractor has fulfilled its obligations completely. The Contractor shall submit the documentation to the Customer without being requested to do so.
- (8) The commissioning of subcontractors who carry out commissioned processing not only from the territory of the EU or EEA shall be possible only if the conditions set out in Chapters 4 (10) and (11) of this Agreement are observed. In particular, it is only permissible as far and as long as the subcontractor offers appropriate data protection safeguards. The Contractor shall inform the Customer of the concrete data protection safeguards offered by the subcontractor and how a

copy of such safeguards can be obtained. Insofar as currently valid standard contractual clauses on the basis of a decision of the EU Commission (e.g., under Commission Decision 2010/87/EU) or standard data protection clauses under Art. 46 GDPR are used as appropriate safeguards, the Controller will give Processor power of attorney to enter into standard data protection clauses adopted by the EU Commission on behalf of Controller. The parties are in agreement that existing standard contractual clauses between the Processor and the subcontractors fulfil the before-mentioned requirement.

- (9) The Contractor shall adequately verify compliance with the subcontractor's obligations on a regular basis, at the latest every 12 months. The audit and its results shall be documented in a comprehensible manner so that they can be understood by a competent third party. The documentation shall be submitted to the Customer without being requested to do so. The Contractor shall keep the documentation on the tests carried out at least until the end of the third calendar year after completion of the contract processing and shall submit it to the Customer at any time upon request.
- (10) If the subcontractor does not comply with its data protection obligations, the Contractor shall be liable to the Customer for this.
- (11) At present, the subcontractors designated in Attachment 2 with their names, addresses and commissioning contents are engaged in the processing of personal data to the extent specified therein and are approved by the Customer. The other obligations of the Contractor towards subcontractors set forth herein shall remain unaffected.
- (12) For the purposes of this Agreement, subcontracting relationships are only those services which are directly related to the performance of the main service. Ancillary services, such as transport, maintenance, cleaning and the use of telecommunications services or user services, are not included. The Contractor's obligation to ensure compliance with data protection and data security in these cases shall remain unaffected.

8 Rights and Obligations of the Customer

- (1) The Customer is solely responsible for assessing the admissibility of the commissioned processing and for safeguarding the rights of data subjects.
 - (2) The Customer places all commissions [orders], partial commissions or instructions in a documented manner. In urgent cases, instructions may be given verbally. The Customer will confirm such instructions with documentation immediately.
 - (3) The Customer shall inform the Contractor without delay if it detects errors or irregularities in the review of the Agreement results.
 - (4) The Customer shall be entitled to monitor compliance with the provisions on data protection and contractual agreements at the Contractor to a reasonable extent itself or through third parties, in particular by obtaining information and inspecting the stored data and data processing programs as well as other on-site inspections. The persons entrusted with the inspection shall be given access and insight by the Contractor to the extent necessary. The Contractor is obliged to provide necessary information, to demonstrate procedures and to provide verification which is necessary for the performance of an inspection. The Contractor shall be entitled to refuse inspections by third parties insofar as they are in a competitive relationship with it or for similarly important reasons.
 - (5) Checks at the Contractor's premises must be carried out without avoidable disruptions to its business operations. Unless otherwise indicated for urgent reasons to be documented by the Customer, inspections shall be carried out after reasonable advance notice and during the Contractor's business hours and not more frequently than every 12 months. Insofar as the Contractor provides verification of the correct implementation of the agreed data protection obligations as provided for in Chapter 5 (8) of this Agreement, a check shall be limited to spot checks.
 - (6) The Contractor shall receive a lump-sum expense allowance of EUR 2,500.00 plus VAT per inspection for the expenses incurred during an on-site inspection. The Customer undertakes to bear the costs actually incurred because of an inspection and exceeding the agreed lump-sum.
-

The Contractor shall provide evidence of the amount of the higher costs actually incurred. In addition, the Contractor shall receive remuneration of EUR 250 per working hour plus VAT if the Client requests additional evaluations, documentation, etc. over and above the test certificates/reports specified in this Agreement.

9 Notification Duties

- (1) The Contractor shall immediately notify the Customer of any violations of the protection of personal data processed on behalf of the Customer. Justified cases of suspicion of this must also be reported. The notification must be sent within 24 hours of the Contractor becoming aware of the relevant event to an address specified by the Customer. It shall contain at least the following information:
 - a. a description of the nature of the breach of the protection of personal data, indicating where possible the categories and approximate number of data subjects, the categories concerned and the approximate number of personal data sets concerned;
 - b. the name and contact details of the Data Protection Officer or any other contact point for further information;
 - c. a description of the likely consequences of the violation of the protection of personal data;
 - d. a description of the measures taken or proposed by the Contractor to remedy the breach of the protection of personal data and, where appropriate, measures to mitigate its possible adverse effects
- (2) Significant disruptions in the execution of the commissioning and violations of data protection provisions or the provisions made in this Agreement by the Contractor or the persons employed by it shall also be notified without delay.
- (3) The Contractor shall inform the Customer without delay of any controls or measures taken by supervisory authorities or other third parties as far as they are related to commissioning processing.
- (4) The Contractor undertakes to assist the Customer in its obligations under Articles 33 and 34 of the GDPR to the extent necessary.

10 Instructions

- (1) The Customer reserves the right to give comprehensive instructions with regard to the processing in the commissioning.
- (2) The Customer and the Contractor shall name the persons exclusively authorized to issue and accept instructions in Attachment 3.
- (3) In the event of a change or a longer-term prevention of the designated persons, successors or representatives must be notified to the other party without delay.
- (4) The Contractor shall inform the Customer immediately if, in the Contractor's opinion, an instruction issued by the Customer violates statutory provisions. The Contractor is entitled to suspend the execution of the corresponding instruction until it is confirmed or changed by the responsible person at the Customer.
- (5) The Contractor must document the instructions given to it and their implementation.

11 Agreement Termination

- (1) If data processed in the commissioning or copies thereof are still in the Contractor's power of disposal at the end of the contractual relationship, the Contractor shall either destroy the data or hand it over to the Customer at the Customer's option. The Customer must make the choice within 2 weeks of being requested to do so by the Contractor. Destruction must be carried out in such a way that it is no longer possible to recover even residual information with justifiable effort.
- (2) The Contractor is obliged to bring about the immediate destruction or return, also in the case of subcontractors.

- (3) The Contractor shall furnish verification of proper destruction and submit such verification to the Customer without delay.
- (4) Documentation which serves as verification of proper data processing shall be kept by the Contractor at least until the end of the third calendar year after the end of the Agreement. It may hand them over to the Customer for liability release.

12 Remuneration

The remuneration of the Contractor is conclusively regulated in the Main Contract. There shall be no separate remuneration or costs reimbursement within the scope of this Agreement.

13 Liability

- (1) The Customer and the Contractor are jointly and severally liable for the compensation of damages suffered by a person due to inadmissible or incorrect data processing within the scope of the contractual relationship.
- (2) The Contractor shall bear the burden of proof that damage is not the result of a circumstance for which it is responsible, insofar as it has processed the relevant data under this Agreement. As long as this proof has not been furnished, the Contractor shall indemnify the Customer upon first request against all claims raised against the Customer in connection with the processing of the commissioning. Under these conditions, the Contractor shall also reimburse the Customer for all costs incurred in legal defense.
- (3) The Contractor shall be liable to the Customer for any damage culpably caused by the Contractor, its employees or its agents or subcontractors employed by the Contractor in connection with the performance of the commissioned contractual services.
- (4) Numbers (2) and (3) shall not apply if the damage has been caused by the correct implementation of the commissioned service or an instruction issued by the Customer.

14 Contractual Penalty

- (1) In the event of culpable breaches of the obligations of this Agreement, the Contractor shall owe a contractual penalty commensurate with the violation. The contractual penalty shall be forfeited in particular in the event of defects in the implementation of the agreed technical and organizational measures. In the case of permanent infringements, each calendar month in which the infringement occurs in whole or in part shall be deemed an individual case. The plea of continuation is excluded.
- (2) The amount of the contractual penalty shall be determined by the Client at its reasonable discretion. If it is unreasonable, it is set by judicial judgement.
- (3) The contractual penalty shall become due when the Customer claims its amount.
- (4) The contractual penalty has no influence on other claims of the Customer.

15 Special Termination Right

- (1) The Customer may terminate the Main Contract and this Agreement at any time without notice ("extraordinary termination") if the Contractor has committed a serious breach of data protection regulations or the provisions of this Agreement, is unable or unwilling to carry out a lawful instruction from the Customer or denies the Customer's rights of control in breach of the Agreement.
- (2) A serious breach shall be deemed to have occurred in particular if the Contractor fails to fulfil or has failed to fulfil to a considerable extent the obligations specified in this Agreement, in particular the agreed technical and organizational measures.
- (3) In the case of insignificant infringements, the Customer shall set the Contractor a reasonable period of time to remedy the situation. If the remedy is not provided in time, the Customer is entitled to extraordinary termination as described in this section.

- (4) The Contractor shall reimburse the Customer for all costs incurred by the latter as a result of the premature termination of the Main Contract or of this Agreement as a result of extraordinary termination by the Customer.

16 Other

- (1) Both parties are obliged to treat confidential all knowledge of business secrets and data security measures of the respective other party acquired within the scope of the contractual relationship, also beyond the termination of the Agreement. If there are doubts as to whether information is subject to confidentiality, it shall be treated as confidential until it is released in writing by the other party.
- (2) Should the Customer's ownership of the Contractor be endangered by measures taken by third parties (e.g., by seizure or confiscation), by insolvency proceedings or settlement proceedings or by other events, the Contractor shall notify the Customer immediately.
- (3) For collateral contracts, the written form and express reference to this Agreement is required.
- (4) Should individual parts of this Agreement be invalid, this shall not affect the validity of the remaining parts of the Agreement.

17 Conclusion of contract

- (1) This contract is concluded electronically and is valid without signature.
(according to § 126b BGB in conjunction with Art. 28 para. 9 DSGVO)

[date]

date

[name of clinic]

[name of practitioner]

Customer

[date]

date

Modern Me GmbH

Gleb Grützner

Contractor

Attachment 1 - Technical and Organizational Measures

In the following, the commissioning-related technical and organizational measures to guarantee data protection and data security are specified, which the Contractor must at least set up and continuously maintain. The aim is to guarantee, in particular, the confidentiality, integrity and availability of the data processed in the commissioning.

Confidentiality (Art. 32 (1)(b) GDPR)

- Physical Access Control
No unauthorized access to data processing systems: Access is controlled via physical keys and surveilled via video systems;
- Electronic Access Control
No unauthorized use of the system: secure passwords manage access to electronic systems, two-factor authentication is in use when applicable, data connections utilize https-SSL-encryption by default, data storage utilizes encryption;
- Internal Access Control
No unauthorized reading, copying, modification or removal within the system: Access is granted on a need-to-know basis. Access level is managed via build-in-rights-management solutions.
- Pseudonymization (Art. 32 (1)(a) GDPR; Art. 25 (1) GDPR)
Pseudonymization ensures processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the involvement of additional information, this additional information is kept separately and subject to need-to-know rights management measures.

Integrity (Art. 32 (1)(b) GDPR)

- Transfer Control
No unauthorized reading, copying, modifying or removing during electronic transmission or transport: Is ensured via data transfer encryption
- Input control
Determining whether and by whom personal data has been entered, modified or removed in data processing systems: Is ensured via build-in-logging-solution and document management.

Availability and Resilience (Art. 32 (1)(b) GDPR)

- Availability Control
Protection against accidental or willful destruction or loss: backup strategy includes redundant, encrypted, off-site, online backups and ensures rapid recoverability.

Procedures for regular review, assessment and evaluation (Art. 32 (1)(d) GDPR; Art. 25 (1) GDPR)

- Data protection management; including the required regular review, assessment and evaluation of data protection measures;
- Incident response management;
- Data protection by design and default settings (Art. 25 (2) GDPR);
- Control of commissioned data processing

Attachment 2 – Approved Subcontractors

- AWS, 26/28 Rue Edward Steichen, 2540 Luxembourg, Luxemburg
- sipgate GmbH, Gladbacher Str. 74, 40219 Düsseldorf, Germany
- Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
- DocuSign Germany GmbH, Neue Rothofstrasse 13-19, 60313 Frankfurt am Main, Germany
- salesforce.com Germany GmbH, Erika-Mann-Str. 31, 80636 München, Germany
- FastBill GmbH, Taunustor 1, 60310 Frankfurt am Main, Germany
- DATEV eG, Paumgartnerstr. 6 – 14, 90429 Nürnberg, Germany

Attachment 3 – Persons Authorized to Give Instructions, Address for Reporting Data Protection Violations

The following persons are authorized to give and receive instructions:

Persons authorised to issue instructions to the Contractor:

[name of practitioner]

Recipients of the Contractor's instructions are:

Mr. Gleb Grützner CEO

Communication channels to be used for instructions:

Benrather Schlossallee 31

40597 Düsseldorf

datenschutz@modern-clear.de

Phone +49 211 97531652

Contact for the notification of personal data breach:

[name of practitioner] of [name of clinic]

Gleb Grützner of Modern Me GmbH

Attachment 4 - Data Protection Officer

Currently, the following person has been appointed as external data protection officer at the Contractor:

DataCo GmbH

Dachauer Street 65

80335 Munich

Germany

+49 89 7400 45840

www.dataguard.de