Order processing pursuant to Art. 28 DS-GVO (German Data Protection Regulation- GDPR)

1. Data Processing in the European Union

The provision of the contractually agreed data processing shall take place exclusively in a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. Any relocation to a third country requires the prior consent of the Client and may only take place if the special requirements of Art. 44 et seq. GDPR are fulfilled.

2. Technical and organisational measures

(1) The Contractor shall document the implementation of the technical and organisational measures required under the GDPR before the start of processing, in particular regarding the specific fulfilment of the contract. These measures are the basis of the order. Should the examination/audit of the Client reveal a need for adaptation, this shall be implemented by mutual agreement.

(2) The precautions to be taken are data security measures aimed at ensuring a level of protection appropriate to the risk in terms of confidentiality, integrity, availability, and resilience of the systems. The state of the art, the implementation costs and the nature, scope, and purposes of the processing as well as the likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32(1) of the GDPR shall be taken into account.

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the contractor is permitted to implement alternative adequate measures. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented.

(4) The Contractor undertakes to implement and further comply with all technical and organisational measures required for this contract in accordance with Art. 28 (3) sentence 2 lit. c, 32 GDPR [details in Annex 1]. The inspection of the technical and organisational measures taken by the Client shall be carried out within the scope of its supervisory powers pursuant to clause 6 of this contract.

3. Correction, restriction, and deletion of data

(1) The contractor may not correct, delete, or restrict the processing of data processed under the contract on its own authority, but only in accordance with documented instructions from the Client. Should a data subject contact the Contractor directly in this regard or regarding other data subject rights, the Contractor shall forward this request to the Client without delay.

(2) If the parties have agreed this separately in a contract, the deletion concept, right to be forgotten, correction, data portability and information shall be ensured directly by the Contractor in accordance with the Client's documented instructions.

4. Further obligations of the contractor

In addition to compliance with the provisions of this Order, the Contractor shall fulfil its statutory obligations under Articles 28 to 33 of the GDPR; in this respect, the Contractor shall in particular ensure compliance with the following requirements:

a) If required by law, a data protection officer shall be appointed in writing to carry out his activities in accordance with Articles 38 and 39 of the GDPR. The contract details of the

Contractor's data protection officer can be found in Section 10 of this Agreement. The Client shall be informed immediately in case of any change of data protection officer.

b) The Contractor undertakes to maintain confidentiality during processing in accordance with Art. 28 (3) sentence 2 lit. b, 29,32 (4) GDPR. When carrying out the work, the Contractor shall use employees who have been obligated to maintain confidentiality and who have been previously familiarised with the data protection provisions relevant to them. The Contractor and any person subordinate to the Contractor who has access to personal data may process such data exclusively in accordance with the Client's instructions, including the power granted in this Contract, unless they are legally obliged to process it by EU law or the Processor's national law.

c) The Client and the Contractor shall cooperate, upon request, with the supervisory authority in the performance of their duties.

d) The Contractor shall inform the Client without delay about control actions and measures of the supervisor authority if they relate to this order.
This shall also apply if a competent authority investigates the Contractor in the context of administrative offence or criminal proceedings regarding the processing of personal data during order processing.

e) To the extent that the Client, for its part, is subject ton an inspection by the supervisory authority, administrative offence or criminal proceeding, the liability claim of a data subject or a third party or any other claim in connection with the order processing at the Contractor, the Contractor shall support it to the best of his ability.

f) The Contractor shall regularly monitor internal processes and technical and organisational measures to ensure that processing within his area of responsibility is carried out in compliance with the requirements of applicable data protection law and that the protection of the rights of the data subject is ensured.

5. Subcontracting relationships

(1) Subcontracting relationships within the meaning of this regulation shall be understood to be services which directly relate to the provision of the main service. This does not include supplementary services which the Contractor uses e.g. as telecommunication services, postal/transport services. However, the Contractor is obliged to take appropriate and legally compliant contractual arrangements as well as control measures in order to ensure data protection and data security of the Client's data, also in the case of outsourced supplementary services.
(2) The Client shall grant the Contractor general authorisation to use further subcontractors if

- a contractual agreement is concluded with the subcontractor in accordance with Article 28 (2-4) of the GDPR,
- the Contractor informs the Client in text form - for example by e-mail/newsletter or via a link - if he intends to use further subcontractors or to replace them.

The Client may object to such changes, whereby this may not be done without an important reason under data protection law. The objection to the intended change must be made in text form to the contact details of the data protection officer stated below under point 10 within 14 days after the information about the change has been provided to the Contractor. In the event of an objection, the Contractor may, at his own discretion, provide the service without the intended change or - if the provision of the service without the intended change is not reasonable for the Contractor - discontinue the service vis-à-vis the Client within 4 weeks after receipt of the objection and terminate the service agreement without notice and with immediate effect.
(3) The transfer of personal data of the Client to the subcontractor and the subcontractor's first activity shall only be permitted once all requirements for subcontracting have been met.
(4) If the subcontractor provides the agreed service outside the EU/EEA, the Contractor shall ensure that it complies with data protection law by taking appropriate measures. The same shall apply if service providers within the meaning of para. 1 sentence 2 are to be employed.

(5) Further outsourcing by the subcontractor requires the express consent of the Contractor (at least in text form) or a general approval of the Contractor analogous to paragraph 2. All contractual provisions in the contractual chain shall also be imposed on the additional subcontractor.

6. Rights of inspection of the Client

(1) The Client shall have the right to carry out inspections in consultation with the Contractor or to have them carried out by inspectors to be named in individual cases. The Client shall have the right to assure itself of the Contractor's compliance with this Agreement in the Contractor's business operations by means of spot checks, which must generally be notified in good time (in principle at least two weeks in advance). Company and business secrets of the Contractor which become known to the Client during an inspection shall be treated as strictly confidential by the Client. No records of such secrets may be made unless this is necessary to exercise the right of inspection on the part of the Client.

(2) The Contractor shall ensure that the Client can convince itself of the Contractor's compliance with its obligations pursuant to Article 28 of the GDPR. The Contractor undertakes to provide the Client with the necessary information upon request and, in particular, to provide evidence of the implementation of the technical and organisational measures.

(3) Evidence of such measures, which do not only concern the specific order, can be provided by current certificates, reports or report extracts from independent bodies (e.g. data protection officer, auditor, audit, IT security department, data protection auditors, quality auditors).

(4) Access to the Contractor's premises shall only take place in the permanent presence of a representative of the Contractor. This representative shall be authorised to decide how the inspection is to proceed to the extent necessary to avoid disruption of the Contractor's business operations and to preserve the Contractor's confidentiality obligations towards third parties.

(5) Regular on-site inspections by the Client are permitted a maximum of once per calendar year. Additional inspections by the Client may only be carried out for an important reason to be proven by the Client.

7. Notification of infringements by the Contractor

Where necessary, in particular because the relevant information is not otherwise available to the Client, and taking into account the nature of the processing, the Contractor shall assist the Client in complying with the personal data security obligations set out in Articles 32 to 36 of the GDPR, data breach notification obligations, data protection impact assessments and prior consultations. These include, but are not limited to:

(a) ensuring an adequate level of protection through technical and organisational measures that consider the circumstances and purposes of the processing as well as the predicted likelihood and severity of a potential security breach and allow for the immediate detection of relevant breach events.

(b) an obligation to notify personal data breaches to the Client without undue delay

(c) the obligation to assist the Client in his duty to inform the data subject and, in this context, to provide the Client with all relevant information without unreasonable delay

(d) to assist the Client in carrying out his data privacy impact assessment

(e) assisting the Client in the context of prior consultations with the supervisory authority.

8. Authority of the Client to issue instructions

(1) The Client shall confirm verbal instructions without delay (at least in text form).

(2) The Contractor shall inform the Client without delay if it is of the opinion that an instruction violates data protection regulations. The Contractor shall be entitled to suspend the implementation of the corresponding instruction until it is confirmed or amended by the Client.

9. Deletion and return of personal data

(1) Copies or duplicates of the data shall not be made without the knowledge of the Client. Exceptions to this are security copies, if they are necessary to ensure proper data processing, as well as data that is required regarding compliance with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier upon request by the Client - at the latest upon termination of the service agreement - the Contractor shall hand over to the Client all documents that have come into its possession, processing and utilisation results produced as well as data files that are related to the contractual relationship or, after prior consent, destroy them in accordance with data protection law, unless the legal provisions of the EU or national law require the storage of personal data.

(3) Documentation which serves as proof of the orderly and proper data processing shall be kept by the Contractor beyond the end of the contract in accordance with the respective retention periods. He may hand them over to the Client at the end of the contract to relieve him of the obligation.

10. Specification of the contract content, subcontractor, and data protection officer

Subject of the contract	The subject of the data handling contract is the execution of the following tasks by the Contractor: • Manufacture of aesthetic dental splint and wire systems (so-called aligners and retainer systems) according to the Client's specifications as well as the manufacture of other medical products. The individual medical products can be found on the website of the Contractor.
Duration of the order	The duration of this order is limited to the duration of the business relationship.
Nature and purpose of the intended processing of data	• The Client shall provide the Contractor with patient data serving as basis for the manufacture of the specific medical device by the Contractor. For this purpose, the Contractor shall provide an internet portal for uploading the necessary patient information. Alternatively, the patient data shall be sent by mail (in particular the sending of the dental impression).
Categories of persons concerned	Patients of the Client

Nature of data	The following types/categories of data are the subject of processing of personal data: • general personal data of the patient (for example: name, date of birth, gender, ID) • health data (for example: diagnostic data, in particular scan/mode of the jaw, patient history, required medical product) • data on implementation of contract • physical characteristics (for example: gender, height, weight).
Subcontractors employed	1. SCHEU-DENTAL GmbH, Am Burgberg 20, 58642 Iserlohn, accounting, 2. Timme Hosting GmbH & Co. KG, Ovelgönner Weg 43,21335 Lüneburg, Hosting Services.
Data protection officer of the Contractor	Dietrich Felgner, mip Consult GmbH, Wilhelm-Kabus-Str. 9, 10829 Berlin, 030-2088999-0, d.felgner@mip-consult.de

Annex 1

Technical and Organisational Measures (TOM)

within the meaning of

Art. 25, 32 of the General Data Protection Regulation (GDPR)

Controller	
Company	SCHEU-DENTAL custom-made GmbH

Address of controller	
Street	Walder Strasse 53
Post code	40724
City	Hilden
Phone	+49 (0)2104 80041 00
Fax	+49 (0)2104 80041 99
E-mail	datenschutz@scheu-dental.com

A. Confidentiality and integrity, Art. 32 (1) lit. b GDPR

I. Entry and access control

Refusal of entry and access to processing systems that are used for the processing activities for unauthorised parties (to the premises and technical systems).

Technical-organisational measures

- Entrances to the premises secured with locking system
    - Security keys with documented key management (key release logbook) for office buildings
- Measures for the prevention and detection of unauthorised access and attempts to gain access through regular checks that the doors, gates, and windows are secured against forced entry
- Separate entry control for the following premises (keys released to authorised persons only on a need-to-know basis) / documented entry / escort:
    - Server
    - Separate backup in 2nd fire area
- Access authorisation to data processing systems and closed networks are limited to the necessary minimum (need-to-know principle)
- Written regulations for employees for the correct and secure use of passwords (adequate password security)
- Reception logbook: Logging visitors, including non-disclosure obligation, Art. 28 (3) S. 2 lit. b, 29, 32 (4) GDPR (previously Section 5 of the Federal Data Protection Act, old version)
- Documented and traceable processes for obtaining, modifying, and returning access authorisations
- Access authorisations are regularly checked to ensure they are up to date and the check is documented
- Securing the network infrastructure with network port security in accordance with IEEE 802.1X, intrusion detection systems, separation of networks (WLAN network is separated from LAN infrastructure, access to internal resources not possible via WLAN), content filters, encrypted network protocols.
- Immediate installation of critical or important security updates / patches
    - in client operating system,
    - in server operating systems that can be reached via public networks (e.g. webservers),
    - in application programs (incl. browsers, plugins, PDF readers etc.), and
    - in security infrastructure (virus scanners, firewalls, IDS systems, content filters, routers, etc.) within 48h from publication by the manufacturer as well as in server operating systems of internal servers within 1 week from publication by the manufacturer.

II. Data carrier control

Prevention of unauthorised reading, copying, modification or deletion of data carriers

Technical-organisational measures
• Logging the authorised transfer of data carriers (external hard drives, USB sticks, memory cards, etc.), • Data carriers that are no longer required are discarded in accordance with data protection laws, • Written regulations for employees on how to handle and ensure the security of mobile devices and data carriers

III. Storage control

Prevention of unauthorised entry of personal data as well as unauthorised reading, modification, and deletion of stored personal data

Technical-organisational measures
• Authorisation concept with needs-based access rights at file system level (controlled by LDAP) • Authorisation concept with needs-based access rights for the software used • Logging all access within the applications used • Physical deletion of data carriers before reuse • Regular check and management of rights by system administrator • Use of file shredders • No use of shared user accounts and/or user access

IV. User control

Prevention of the use of automated processing systems with the help of facilities for data transfers by unauthorised persons

Technical-organisational measures
• Individual user Ids and passwords are required for using the systems • Written regulations for employees regarding the correct use of passwords (adequate password security); when using passwords for authentication, consistent password quality of at least 8 characters, 3 levels of complexity and a maximum change interval of 180 days is ensured. • Use of automatic locking mechanisms • Obligation of employees to log out from and/or block the system when leaving the workstation • Multiple entry of incorrect access data prohibited • Access is granted in accordance with management's instructions and/or according to individual decisions made by management • Access authorisations are regularly checked to ensure they are up to date and the check is documented • Forcing secure passwords in all applications via application and/or LDAP

V. Access control

Ensuring that the persons authorised to use an automated processing system only have access to the personal data covered by their access authorisation

Technical-organisational measures

- Access authorisations are regularly checked to ensure they are up to date and the check is documented
- Effective control of the access authorisations through an adequate authorisation and role concept
- Restriction of the access authorisations for order data to the absolute minimum required (need-to-know principle, least privilege principle)
- Documented and traceable processes for obtaining, modifying, and returning access authorisations
- Logging all access to applications, incl. administrators
- Measures for protecting devices, servers, and other infrastructure components against unauthorised access: anti-virus concept, content filters, application firewall, intrusion detection system

VI. Transfer control

Ensure that it is possible to verify and establish to which points personal data have been or may be transmitted or made available by means of data communication equipment

Technical-organisational measures

- Outgoing connections are protected
- Network input / output points are documented
- Access to systems in which personal data is processed only via encrypted connections.
- AES encryption via AES-256 for access to customer/patient data
- Definition of secure transfer paths only (HTTPS protocol)
- HSTS headers via Helmet (Prod/Test/Test2)
- Data transfer via FTPS
- System administration via SSH
- Passwords in accordance with password Policy (8 characters, letters, numbers, special characters)
- IPSEC / L2TP (PSK) for VPN connections

VII. Input control

Ensuring that it is possible to subsequently check and determine which personal data was entered or modified in automated processing systems at which time and by whom

Technical-organisational measures

- Logging the input, modification, and deletion of personal data as well as traceability based on individual usernames
- Only specifically defined employees have access to systems containing personal data (restriction of persons who input data)
- No use of group accounts (also administrators or root) and/or one account by several employees
- Granting authorisations to individual users for entering, modifying, and deleting data

VIII. Transport control

Ensuring that both confidentiality and integrity of personal data are protected when transferring personal data and when transporting data carriers

Technical-organisational measures
• Setting up VPN tunnels • TLS protocol for sending e-mails • Securing the network infrastructure with network port security in accordance with IEEE 802.1X, intrusion detection system, network separation, content filters, encrypted network protocols • Use of encrypted transfer protocols (e.g. SSL-based protocols)

IX. Data integrity

Ensuring that stored personal data cannot be damaged by system errors

Technical-organisational measures
• Backup mechanisms (at regular intervals) and documentation of the recovery mechanism • Disaster recovery plan and corresponding tests (particularly that backups can be reinstalled)

X. Separability

Ensuring that personal data collected for different purposes can be processed separately

Technical-organisational measures
• Physically separate storage in separate systems or data carriers (depending on purpose) and/or in different access areas and/or folders with corresponding access authorisations • Logical and/or physical separation of test, development, and production systems

XI. Pseudonymisation and encryption measures, Art. 32 (1) lit. a, Art. 25 (1) GDPR

Pseudonymisation: The processing of personal data in such manner that the data can no longer be allocated to one specific data subject without referring to additional information. Details may have to be specified when listing the processing activities.

Technical-organisational measures
• Regular check which data can be anonymised and/or deleted

B. Availability and resilience, Art. 32 (1) lit. b GDPR

I. Quick recoverability, Art. 32 (1) lit. c GDPR

Ensuring that the systems used can be recovered quickly in the event of breakdown

Technical-organisational measures
• Backup and recovery concept, particularly automatic backups • Storage of data backups in a second fire area • Data backup testing

II. Reliability

Ensuring that all system functions are available, and malfunctions are reported

Technical-organisational measures
• System monitoring (automatically and manually) • Error log handling • Server storage monitoring

III. Availability control

It must be ensured that personal data is protected against deliberate or accidental destruction as well as loss.

Technical-organisational measures
• Uninterrupted power supply (UPS) • Operation and regular maintenance of server rooms by IT • Backup storage in separate and protected premises • Daily backups • Regular check of the backups for data recoverability • Processes and documentation for recovering systems and data

C. Methods for regular checks, assessment, and evaluation; Art. 32 (1) lit. d, Art. 25 (1) GDPR

I. Data protection management

- A data protection officer has been appointed in writing:
  - Dietrich Felgner, lawyer, mip Consult GmbH, Wilhelm-Kabus-Strasse 9, 10829 Berlin, Germany, d.felgner@mip-consult.de, tel. +49 30 20 88 999 0
  - The data protection officer has provided proof of his professional qualifications.
- The employees are made aware of the topic of data protection in regularly offered training sessions.

- Proof has been provided that all employees have been obliged to maintain data secrecy.
    - Information and awareness-raising measures are being implemented on a regular basis to raise awareness about data protection and the law.
- Processing activities are recorded in a list that is continuously being updated.
- The following documentation has been provided.
    - Technical-organisational measures, see this document
    - Written work instructions / guidelines / leaflets
- A concept for the regular check, assessment, and evaluation of the effectiveness of the technical and organisational measures to ensure the security of the processing activities has been implemented. In particular, a review of the technical and organisational measures is performed once a year with the responsible IT employees and the corresponding steps formulated, tracked and documented in the annual report.
- The storage of the protocols relating to data protection matters has been arranged.
- Advance controls in accordance with Section 4d BDSG and/or assessments of the consequences in accordance with Art. 35 GDPR are implemented and logged.
- Contact person for information in accordance with Art. 15 GDPR and additional rights in accordance with GDPR: datenschutz@scheu-dental.com
- Occasional, unannounced checks of the compliance with data protection and data security measures are being performed.

Albert Sterkenburg

✓ Certified by yousign

Rüdiger Schmidt

✓ Certified by yousign