Version 1.7

Contract Data Processing Agreement

between

Client regarding General terms and Conditions

of PracticeDent Data Processing

– Client –

and

Medicloud AG
Amlehnstrasse 22
6010 Kriens

– Contractor –

1. General points

(1) The Contractor processes personal data on behalf of the Client as defined by Art. 4 No. 8 and Art. 28 of Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). This Agreement regulates the rights and obligations of the parties in connection with the processing of personal data.

(2) Where the terms "data processing" or "processing" (of data) are used in this Agreement, the definition of "processing" as defined by Art. 4 No. 2 GDPR shall apply.

2. Subject of the order

The subject of the processing, the type and purpose of the processing, the type of personal data and the categories of data subjects are defined in **Annex 1** to this Agreement.

3. Rights and obligations of the Client

(1) The Client is the party responsible for the processing of data on behalf of the Contractor as defined by Art. 4 No. 7 GDPR. According to Clause 4, paragraph 5, the Contractor has the right to inform the Client if the order and/or instructions involve data processing which it considers legally unacceptable.

(2) As the responsible party, the Client is responsible for safeguarding the rights of data subjects. The Contractor shall inform the Client immediately if the data subjects assert their rights against the Contractor.

(3) The Client has the right to issue additional instructions to the Contractor at any time regarding the type, scope and procedures of data processing. Instructions must be given in text form (e.g. by email).

(4) This shall be without prejudice to any provisions regarding any compensation for additional expenses arising from supplementary instructions given to the Contractor by the Client.

(5) The Client can name persons authorised to issue instructions. If persons entitled to issue instructions are to be appointed, they will be named in **Annex 1**. In the event that the persons authorised to issue instructions with the Client change, the Client shall inform the Contractor of this in text form.

(6) The Client shall immediately inform the Contractor if it detects errors or irregularities in connection with the Contractor's processing of personal data.

(7) In the event that there is an obligation to inform third parties pursuant to Articles 33, 34 DSGVO or any other statutory reporting obligation applicable to the Client, the Client shall be responsible for compliance therewith.

4. General obligations of the Contractor

(1) The Contractor processes personal data exclusively within the scope of the agreements made and/or in compliance with any additional instructions given by the Client. Exceptions to this are legal regulations which may oblige the Contractor to process the goods elsewhere. In such a case, the Contractor shall notify the Client of these legal requirements prior to processing, unless the law in question prohibits such notification for reasons of substantial public interest. The purpose, type and scope of data processing are otherwise based exclusively on this Agreement and/or the instructions of the Client. Any processing of data by the Contractor that deviates from this is prohibited, unless the Client has agreed to the same in writing.

(2) The Contractor undertakes to carry out the contract data processing only in member states of the European Union (EU) or the European Economic Area (EEA).

(3) The Contractor guarantees that all agreed measures relating to the processing of personal data in accordance with the order shall be processed in a contractually compliant way.

(4) The Contractor is obliged to design its company and operating processes such that the data, which it processes on behalf of the Client, are protected to the required extent and that any unauthorised access by third parties is prevented. The Contractor shall agree any changes in the organisation of the contract data processing which impact on the security of the data with the Client in advance.

(5) The Contractor shall inform the Client immediately if it considers that any instructions given by the Client violate legal regulations. The Contractor is entitled to suspend the execution of the relevant instruction until confirmed or changed by the Client. If the Contractor can demonstrate that processing in accordance with the instructions of the Client may render the Contractor liable pursuant to Art. 82 GDPR, the Contractor shall have the right to suspend further processing in this respect until the liability between the parties has been clarified.

(6) The processing of data on behalf of the Client outside the Contractor's or subcontractors' premises is only permitted with the consent of the Client in writing or in text form. The processing of data on behalf of the Client within private residences is only permitted with the consent of the Client in writing or in text form.

(7) The Contractor shall process the data that it processes on behalf of the Client separately from other data. Physical separation is not absolutely crucial in this respect.

(8) The Contractor may provide the Client with details of the person(s) who is/are authorised to receive instructions from the Client. If persons authorised to issue instructions are to be appointed, they will be named in **Annex 1**. In the event that the persons authorised to receive instructions for the Contractor should change, the Contractor shall inform the Client of this in text form.

5. Data Protection Officer of the Contractor

(1) The Contractor confirms that it has appointed a data protection officer in accordance with Art. 37 GDPR. The Contractor shall ensure that the Data Protection Officer has the necessary qualifications and expertise. The Contractor shall inform the Client separately in text form of the name and contact details of its data protection officer.

(2) The obligation to appoint a data protection officer in accordance with paragraph 1 may be waived at the discretion of the Client if the Contractor can prove that it is not legally obliged to appoint a data protection officer and the Contractor can prove that operational regulations exist which guarantee the processing of personal data in compliance with the statutory regulations, the provisions of this Agreement and any further instructions of the Client.

6. Reporting obligations of the Contractor

(1) The Contractor is obliged to inform the Client immediately of any violation of data protection regulations or of the contractual agreements made and/or of the instructions given by the Client in the course of the processing of data by the Contractor itself or by other persons involved in said processing. The same applies to any violation of the protection of personal data that the Contractor processes on behalf of the Client.

(2) Furthermore, the Contractor shall inform the Client without delay if a supervisory authority acts vis-à-vis the Contractor pursuant to Art. 58 GDPR and this may also concern any monitoring of the processing that the Contractor performs on behalf of the Client.

(3) The Contractor is aware that the Client may be subject to a reporting obligation pursuant to Articles 33, 34 GDPR, which imposes the obligation to report information to the supervisory authority within 72 hours of becoming aware thereof. The Contractor shall support the Client in implementing the reporting obligations. In particular, the Contractor shall inform the Client immediately of any unauthorised access to personal data processed on behalf of the Client, but no later than 48 hours after becoming aware of said access. Any such notification by the Contractor to the Client must include the following information in particular:

- a description of the nature of the breach of the protection of personal data, indicating, as far as possible, the categories and approximate number of data subjects, the categories concerned, and approximate number of personal data records concerned;
- a description of the measures taken or proposed by the Contractor to remedy the violation of the protection of personal data and, where appropriate, measures to mitigate possible adverse effects.

7. Cooperation obligations of the Contractor

(1) The Contractor supports the Client in its obligation to respond to applications for the protection of rights of data subjects in accordance with Art. 12-23 GDPR. The provisions of Clause 11 of this Agreement shall apply.

(2) The Contractor participates in the creation of directories of processing activities by the Client. It must provide the Client with the information required in this respect in an appropriate way.

(3) The Contractor shall assist the Client in complying with the obligations set out in Articles 32-36 GDPR, taking into account the type of processing and the information available to it.

8. Monitoring powers

(1) The Client has the right at any time to monitor the Contractor's compliance with the legal provisions on data protection and/or compliance with the contractual regulations between the parties and/or the Contractor's instructions to the required extent.

(2) The Contractor is obliged to provide the Client with information insofar as this is necessary to carry out the monitoring within the meaning of paragraph 1.

(3) The Client may request inspection of the data processed by the Contractor for the Client as well as the data processing systems and programs used.

(4) After prior registration and with a reasonable period of notice, the Client may carry out the monitoring as defined by paragraph 1 by conducting an inspection at the Contractor's business premises during normal business hours. The Client shall ensure that such monitoring inspections are carried out only to the extent necessary to avoid any disproportionate disruption to the Contractor's operations.

(5) The Contractor is obliged to provide the Client with the necessary information in the event of measures taken by the supervisory authority against the Client as defined by Art. 58 GDPR, particularly concerning information and monitoring obligations and to enable the relevant supervisory authority to carry out on-site monitoring inspections. The Client must be informed by the Contractor of any planned measures.

9. Subcontracting relationships

(1) Subcontractors may only be commissioned by the Contractor in text form with the consent of the Client. The Contractor shall specify all subcontracting relationships

already existing at the time of conclusion of the Agreement in **Annex 2** to this Agreement.

(2) The Contractor shall carefully select the subcontractor and check before commissioning that the subcontractor can comply with the agreements made between the Client and Contractor. In particular, the Contractor must monitor in advance and regularly during the contractual term that the subcontractor has taken the technical and organisational measures required under Art. 32 GDPR to protect personal data. The Contractor must document the result of the monitoring inspection and send it to the Client on request.

(3) The Contractor is obliged to obtain confirmation from the subcontractor that it has appointed an operational data protection officer in accordance with Art. 37 GDPR. In the event that no data protection officer has been appointed by the subcontractor, the Contractor shall inform the Client accordingly and provide information to the effect that the subcontractor is not legally obliged to appoint a data protection officer.

(4) The Contractor shall ensure that the regulations agreed in this Agreement and any supplementary instructions of the Client are also imposed on the subcontractor.

(5) The Contractor shall conclude an order processing agreement with the subcontractor which meets the requirements of Art. 28 GDPR. In addition, the Contractor shall impose on the subcontractor the same personal data protection obligations as those established between the Client and Contractor. A copy of the Contract Data Processing Agreement must be sent to the Client upon request.

(6) The Contractor is particularly obliged to ensure through contractual regulations that the monitoring powers (Section 8 of this Agreement) of the Client and of supervisory authorities also apply vis-à-vis the subcontractor and that corresponding monitoring rights are agreed by the Client and supervisory authorities. It must also be stipulated in the Agreement that the subcontractor must tolerate these monitoring measures and any on-the-spot inspections.

(7) Subcontracting relationships as defined by paragraphs 1 to 6 shall not be regarded as services which the Contractor commissions from third parties purely as an ancillary service to carry out the business activity. These include, for example, cleaning services, pure telecommunications services without specific reference to services that the Contractor provides for the Client, postal and courier services, transport services, security services. The Contractor is nevertheless obliged to ensure that appropriate precautions and technical and organisational measures have been taken to ensure the protection of personal data, even in the case of ancillary services provided by third parties. The maintenance and servicing of IT systems or applications constitutes a subcontracting relationship and order processing subject to approval as defined by Art. 28 GDPR if the maintenance and testing concerns IT systems which are also used in connection with the provision of services for the Client and which are also accessible during the maintenance of personal data processed on behalf of the Client.

10. Obligation to maintain confidentiality

(1) When processing data for the Client, the Contractor is obliged to maintain confidentiality with regard to data that it has received or of which is has gain knowledge in connection with the order. The Contractor undertakes to observe the same confiden-

tiality rules as are incumbent upon the Client. The Client is obliged to inform the Contractor of any special confidentiality rules.

(2) The Contractor provides an assurance that it is aware of the applicable data protection regulations and is familiar with their application. The Contractor further warrants that it has ensured its employees are familiar with the data protection provisions relevant to them and are bound to confidentiality. The Contractor further warrants that it has, in particular, ensured that the employees tasked with duties for the work project in question are bound to confidentiality and informed them of the instructions of the Client.

(3) Proof of the obligation of the employees to maintain confidentiality as specified in paragraph 2 must be proven to the Client on request.

11. Safeguarding the rights of data subjects

(1) The Client is solely responsible for the protection of the rights of data subjects. The Contractor is obliged to support the Client in its duty to process applications from data subjects according to Art. 12-23 GDPR. In particular, the Contractor shall ensure that the relevant information required is provided to the Client promptly, so that the Client can in particular fulfil its obligations under Art. 12 para. 3 GDPR.

(2) Insofar as the Contractor's cooperation is necessary for the Client to safeguard the rights of data subjects – particularly with regard to information, correction, blocking or deletion – the Contractor shall take the necessary measures in accordance with the Client's instructions. If possible, the Contractor shall support the Client with suitable technical and organisational measures in fulfilling its obligation to respond to requests for the protection of the rights of data subjects.

(3) This shall be without prejudice to any provisions regarding any compensation for additional expenses incurred by the Contractor through provision of cooperation services in connection with assertion of rights of data subjects vis-à-vis the Client.

12. Non-disclosure obligations

(1) Both parties undertake to treat all information received in connection with the execution of this Agreement as indefinitely confidential and to use the same only for the execution of the Agreement. Neither party is entitled to use this information, in whole or in part, for any purposes other than those just mentioned or make it accessible to third parties.

(2) The above obligation does not apply to information which one of the parties has demonstrably received from third parties without being subject to a non-disclosure obligation or which is already in the public domain.

13. Remuneration

The remuneration of the Contractor shall be separately agreed.

14. Technical and organisational data security measures

(1) The Contractor undertakes to the Client that it will comply with the technical and organisational measures required to comply with the applicable data protection regulations. This particularly includes the provisions of Art. 32 GDPR.

(2) The technical and organisational measures in place at the time of conclusion of the Agreement are attached to this Agreement as **Annex 3**. The parties agree that changes in technical and organisational measures may be necessary to adapt to technical and legal circumstances. Significant changes that may affect the integrity, confidentiality or availability of personal data will be agreed by the Contractor with the Client in advance. Measures that entail only minor technical or organisational changes and do not adversely affect the integrity, confidentiality and availability of the personal data can be implemented by the Contractor without consultation with the Client. The Client can request an up-to-date version of the technical and organisational measures taken by the Contractor at any time.

(3) The Contractor shall regularly and occasionally check the effectiveness of the technical and organisational measures taken. In the event that there is a need for optimisation and/or change, the Contractor shall inform the Client.

15. Duration of order

(1) The Agreement shall come into effect when signed and shall be concluded for an indefinite period.

(2) It can be terminated at the end of the quarter with three months' notice.

(3) The Client may terminate the Agreement at any time without notice if there is a serious breach by the Contractor of the applicable data protection regulations or obligations under this Agreement, if the Contractor is unable or unwilling to comply with instructions given by the Client or if the Contractor refuses access to the Client or the competent supervisory authority in breach of the Agreement.

16. Termination

(1) Upon termination of the Agreement, the Contractor shall return to the Client, at the Client's discretion, or delete, all documents, data and processing or usage results that have come into its possession in connection with the contractual relationship. The deletion shall be confirmed via suitable means. Any statutory retention obligations or other obligations to store the data remain unaffected. Data carriers must be destroyed in the event that deletion is requested by the Client, in which case security level 3 of DIN 66399 must be observed as a minimum; the destruction must be verified to the Client with reference to the security level in accordance with DIN 66399.

(2) The Client has the right to ascertain the complete and contractual return and deletion of the data to the Contractor. This can also be done by inspecting the data processing systems at the Contractor's premises. The on-site inspection shall be announced by the Client within a reasonable period of time.

17. Right to retention

The parties agree that the defence of the right of retention by the Contractor is excluded with regard to the processed data and the associated data carriers.

18. Final provisions

(1) Should the Contractor's property be put at risk by measures of third parties (such as seizure or confiscation), insolvency proceedings or other events, the Contractor shall inform the Client promptly. The Contractor shall immediately inform the creditors of the fact that data are being processed on behalf of the Contractor.

(2) Ancillary agreements must be made in writing.

(3) Should individual parts of this Agreement be invalid, this shall not affect the validity of the remaining provisions of the Agreement.

(4) This agreement comes into place if the Client uses the Contractors website and services and has not to be signed personally.

, on	, on
Place date	Place date
______________________	______________________
- Client -	- Contractor -

Annex 1 – Subject of the order

1. Subject and purpose of the processing

The Client's order to the Contractor includes the following work and/or services:

Operation of a web shop, processing of customer data, processing of personal data

2. Type(s) of personal data

The following types of data are regularly processed:

Customer data

Newsletter: Name, E-Mail address, customer number, role

Internal and external reporting: Name, address, E-Mail address, phone number, role

Dispatch of print media: Name, address, E-Mail address, phone number, customer number, role

3. Categories of data subject

Group of data subjects:

customers, clients, third parties, employees

4. Persons authorised to issue instructions for the Client

The Owner

5. Persons authorised to receive instructions for the Contractor

Tino Brantschen, Mathias Riechsteiner

Annex 2 – Subcontractors

The *Contractor* uses the services of third parties who process data on behalf of the Client ("subcontractors").

The scope includes the following company/companies:

Curaden AG, Amlehnstr. 22 6010 Kriens

oneweb GmbH, Brandgässli 6, 6004 Luzern

BitHawk AG, Allee 1A, 6210 Sursee

AnalytikData Prime GmbH, Hauptstrasse 26, 5273 Oberhofen

BitStone SRL, Calea Turzii 36, Cluj-Napoca 400000, Romania

Annex 3
Technical and organisational measures of the Contractor

At Medicloud AG, the following technical and organizational
data security measures within the meaning of Art. 32 GDPR have been taken:

1. Confidentiality

Entrance control

The offices of Medicloud AG are located in an office building in Kriens CH.

The access to the office building and also to the offices of Medicloud AG are locked day and night. Access to the office building is restricted only to the Landlords and tenants of office space. There comes an electronic locking system, which is managed by the landlord. However, each tenant of the office building has the option of administering the transponder keys handed over and of granting and withdrawing electronic access rights. This is managed by Medicloud AG's human resources department.

Key allocation and key management are performed according to a defined process, which regulates the granting and withdrawal of access authorizations for rooms both at the beginning and at the end of an employment relationship.

Allowances shall be issued taking into account the principle of necessity.

Visitors are only granted access to the office building and then to the office building after the door has been opened. The reception can see the entrance door and ensures that every visitor reports to the reception.

Each visitor is recorded in a visitor's book and then accompanied by the receptionist to his respective contact person.

Visitors are not allowed to move freely in the offices unaccompanied.

The entrances and windows of the office building as well as the offices are secured by an alarm system. This can be activated and deactivated manually. Irrespective of this, the alarm system is automatically activated at 9 p.m. every day.

Admission control

The following measures have been taken by Medicloud AG for access control:

In order to gain access to IT systems, users must have the appropriate access authorization. For this purpose, appropriate.

User authorizations are assigned by administrators. However, this only applies if this has been requested by the respective superior. The application can also be made via the personnel department.

The user then receives a user name and an initial password, which must be changed when logging on for the first time. The password defaults contain a minimum password length of 8 characters, whereby the password must insist on upper/lower case letters, numbers and special characters.

Passwords are changed every 90 days. Passwords with a minimum length of 32 characters are excluded. An automatic password change is not indicated here. A password history is stored. This ensures that the past 10 passwords cannot be used again.

Incorrect login attempts are logged. If an incorrect entry is made 3 times, the respective user account is blocked.

Remote access to Medicloud AG IT systems always takes place via encrypted connections.

Medicloud AG servers are equipped with an intrusion prevention system. All server and client systems are equipped with virus protection software, which guarantees a daily updated supply of signature updates. All servers are protected by firewalls, which are always maintained and supplied with updates and patches.
The access of servers and clients to the Internet and the access to these systems via the Internet is also secured by firewalls. This also ensures that only the ports required for the respective communication can be used. All other ports are blocked accordingly.

All employees are instructed to lock their IT systems when they leave them.

Passwords are always stored in encrypted form.

Access control

Authorizations for Medicloud AG IT systems and applications are set up exclusively by administrators.
Authorizations are always assigned according to the Need-to-Know principle. Accordingly, only those persons are granted access rights to data, databases or applications who maintain and maintain these data, applications or databases or are active in development.

The prerequisite for this is a corresponding request for an employee's authorizatio n by a superior. The application can also be submitted to the personnel department.

There is a role-based authorization concept with the option of differentiated assignment of access authorizations, which ensures that employees receive access rights to applications and data depending on their respective area of responsibility and, if necessary, on a project-based basis.

The destruction of data media and paper is carried out by a service provider who guarantees destruction in accordance with DIN 66399.

All employees at Medicloud AG are instructed to deposit information with personal data and/or information about projects in the destruction containers designated for

this purpose. Employees are generally prohibited from installing unauthorized software on IT systems.
All server and client systems are regularly updated with security updates.

Separation

All IT systems used by Medicloud AG for customers are multi-client capable. The separation of data from different customers is always guaranteed.

Pseudonymization & Encryption

Administrative access to server systems is always via encrypted connections.
In addition, data is stored on server and client systems on encrypted data carriers. There are corresponding

Hard disk encryption systems in use.

2. Integrity

Data input control

The input, modification and deletion of personal data processed by Medicloud AG on behalf of Medicloud AG will be recorded.

Employees are obliged to always work with their own accounts. User accounts may not be shared with other persons.

Transfer control

A passing on of personal data, which takes place on behalf of customers of Medicloud AG, may only take place to the extent as agreed with the customer or as far as this is necessary for the provision of the contractual services for the customer.

All employees who work in a customer project are instructed with regard to the permissible use of data and the modalities of passing on data.

As far as possible, data will be transmitted to the recipient in encrypted form. Medicloud AG employees are prohibited from using private data carriers in connection with customer projects.

Medicloud AG employees are regularly trained in data protection topics. All employees are obliged to treat personal data confidentially.

3. Availability and reliability

Data on Medicloud AG server systems are backed up incrementally at least daily and "fully" weekly. The backup media are encrypted and brought to a physically separate location.

The import of backups is tested regularly.

The IT systems have an uninterruptible power supply. The server room is equipped with a fire alarm system and a CO2 extinguishing system.
All server systems are subject to monitoring, which immediately triggers reports to an administrator in the event of malfunctions.

Medicloud AG has an emergency plan, which also includes a restart plan.

4. Procedures for regular review, evaluation and evaluation

Medicloud AG has implemented a data protection management system. There is a guideline on data protection and data security and guidelines with which the implementation of the objectives of the guideline is guaranteed.

The Data Protection and Information Security Team (DST) has been established to plan, implement, evaluate and adapt measures in the area of data protection and data security.

The effectiveness of the guidelines is regularly evaluated and adapted.

In particular, it is ensured that data protection incidents are identified by all employees and immediately reported to the DST. The DST will investigate the incident immediately. As far as data are concerned which are processed on behalf of customers, it is ensured that they are informed immediately about the type and extent of the incident.

When processing data for own purposes, if the requirements of Art. 33 GDPR are met, a report will be made to the supervisory authority within 72 hours of becoming aware of the incident.

Order control

The processing of data takes place exclusively within the European Union.

Medicloud AG has appointed a company data protection officer.
If external service providers or third parties are involved, an order processing contract will be concluded in accordance with the applicable data protection law after a previously conducted audit by the Medicloud AG data protection officer.
Contractors are also checked regularly during the contractual relationship.

Data protection through technology design and data protection-friendly default settings

Medicloud AG already takes care during the development of the software that the principle of necessity is taken into account in connection with user interfaces. For example, form fields and screen masks can be flexibly designed. Mandatory fields can be provided, or fields can be deactivated.

Medicloud AG's software supports both input control through a flexible and adaptable audit trail, which enables unchangeable storage of changes to data and user authorizations.
Authorizations for data or applications can be set flexibly and granularly.