General Terms and Conditions for data processing activities between the Client using the Service, as data controller, and Ceph Assistant Kft., as data processor

CHAPTER I

Condition 1

Purpose and Scope

(a) The purpose of these general terms and conditions (hereinafter referred to as the Terms) is to comply with Article 28(3) and (4) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(b) The data controllers and data processors listed in Annex I have accepted these Terms to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679.

(c) These Terms apply to the processing of personal data specified in Annex II.

(d) Annexes I–IV form an integral part of these Terms.

(e) These Terms do not affect the obligations of the data controller under Regulation (EU) 2016/679.

(f) These Terms alone do not ensure compliance with the obligations related to international data transfers under Chapter V of Regulation (EU) 2016/679.

Condition 2

Immutability of the Terms

(a) The parties agree not to modify the Terms, except to supplement the annexes with additional information or to update the information contained therein.

(b) This does not prevent the Parties from incorporating the general terms and conditions set out in these terms into a broader contract or supplementing them with other clauses or additional safeguards, provided that these do not directly or indirectly contradict these Terms and do not reduce the fundamental rights or freedoms of the data subjects.

Condition 3

Interpretation

(a) Where these Terms use concepts defined in Regulation (EU) 2016/679, the meaning of these concepts shall be the same as in the said Regulation.

(b) These Terms shall be interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Terms shall not be interpreted in a way that contradicts the rights and obligations defined in Regulation (EU) 2016/679, or in a manner that infringes the fundamental rights or freedoms of the data subjects.

Condition 4

Hierarchy

In the event of a conflict between these Terms and the provisions set out in related agreements concluded between the Parties at the time of acceptance of these Terms or thereafter, these Terms shall prevail.

Condition 5

Condition of Accession

(a) Any legal entity that is not a party to these Terms may join these Terms as a data controller or data processor at any time with the consent of all Parties by completing the annexes and signing Annex I.

(b) Following the completion and signing of the annexes referred to in point (a), the acceding legal entity shall be considered a party to these Terms and shall have the rights and obligations of a data controller or data processor in accordance with the designation in Annex I.

(c) The acceding legal entity shall not have any rights or obligations arising from these Terms for the period prior to becoming a party.

CHAPTER II

OBLIGATIONS OF THE PARTIES

Condition 6

Description of the Data Processing

The details of the data processing operations, particularly the categories of personal data and the purposes for which the personal data are processed on behalf of the data controller, are set out in Annex II.

Condition 7

Obligations of the Parties

7.1. Instructions

(a) The data processor shall process personal data only based on the written instructions of the data controller, except when the processing is required by Union or Member State law applicable to the data processor. In such a case, the data processor shall inform the data controller of that legal requirement before processing unless that law prohibits such information on important grounds of public interest. The data controller may issue further instructions throughout the duration of the personal data processing. These instructions must always be documented.

(b) The data processor shall immediately inform the data controller if, in its opinion, an instruction given by the data controller infringes Regulation (EU) 2016/679 or applicable Union or Member State data protection provisions.

7.2. Purpose limitation

The data processor shall process personal data only for the specific purpose(s) set out in Annex II unless further instructions are received from the data controller.

7.3. Duration of personal data processing

The data processor shall process personal data only for the period specified in Annex II.

7.4. Security of data processing

(a) The data processor shall implement at least the technical and organizational measures specified in Annex III to ensure the security of personal data. This includes protecting the data against breaches of security that could result in accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access (data breach). When evaluating the appropriate level of security, the Parties must duly consider the state of the art, implementation costs, the nature, scope, context, and purposes of the data processing, as well as the risks to the data subjects.

(b) The data processor shall provide access to personal data under processing to its employees only to the extent strictly necessary for the execution, management, and monitoring of the contract. The data processor shall ensure that persons authorized to process personal data are subject to confidentiality obligations or are under appropriate confidentiality obligations based on legal requirements.

7.5. Sensitive data

(a) If the data processing involves special categories of personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data aimed at uniquely identifying a natural person, data concerning health, a person's sex life or sexual orientation, or data relating to criminal convictions and offenses (“sensitive data”), the data processor shall apply specific restrictions and/or additional safeguards.

7.6. Documentation and compliance

(a) The Parties must demonstrate compliance with their obligations under these Terms.

(b) The data processor shall promptly and appropriately address any questions from the data controller related to data processing performed in accordance with these Terms.

(c) The data processor shall provide the data controller with all information necessary to verify compliance with obligations directly arising from Regulation (EU) 2016/679 as outlined in these Terms. Upon request, the data processor must also facilitate and contribute to inspections at reasonable intervals or when there are indications of non-compliance with these Terms regarding data processing activities. When deciding on the review or audit, the data controller may consider relevant certifications held by the data processor.

(d) The data controller may choose to conduct the audit itself or engage an independent auditor. Audits may include inspections at the data processor’s premises or physical facilities, which should be carried out with reasonable notice, as applicable.

(e) Upon request, the Parties shall provide the relevant information mentioned in this clause, including the results of audits, to the competent supervisory authority(ies).

7.7. Use of sub-processor

(a) **GENERAL WRITTEN AUTHORIZATION**: The data processor has the data controller's general authorization to engage additional sub-processors. The data processor shall provide the data controller with the information necessary for the data controller to exercise its right to object.

(b) If the data processor engages another sub-processor to carry out specific data processing activities (on behalf of the data controller), it must do so through a contract that imposes on the sub-processor essentially the same data protection obligations as those set out in these Terms for the data processor. The data processor shall ensure that the sub-processor fulfills the obligations applicable to the data processor under these Terms and Regulation (EU) 2016/679.

(c) At the request of the data controller, the data processor must provide a copy of the agreement with the sub-processor and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data processor may redact the agreement before sharing the copy.

(d) The data processor remains fully liable to the data controller for the performance of the sub-processor's obligations under the data processor's contract with the sub-processor. The data processor shall inform the data controller if the sub-processor fails to meet its contractual obligations

(e) The data processor shall include in its agreement with the sub-processor a clause regarding third-party beneficiary rights, which allows the data controller to terminate the contract with the sub-processor and instruct the sub-processor to delete or return personal data if the data processor is actually dissolved, ceases to exist under the law, or becomes insolvent.

7.8. International data transfers

(a) Data transfers by the data processor to a third country or an international organization may only take place based on documented instructions from the data controller or to fulfill a specific requirement of Union or Member State law applicable to the data processor, and must be carried out in accordance with Chapter V of Regulation (EU) 2016/679.

(b) The data controller agrees that if the data processor, in accordance with condition 7.7, engages another sub-processor to perform specific data processing activities (on behalf of the data controller) and these processing activities involve the transfer of personal data under Chapter V of Regulation (EU) 2016/679, the data processor and the sub-processor may ensure compliance with Chapter V of Regulation (EU) 2016/679 by applying the standard contractual clauses adopted by the Commission in accordance with Article 46(2) of Regulation (EU) 2016/679, provided that the conditions for applying those standard contractual clauses are met.

(c) The data processor shall not transfer personal data processed on behalf of the data controller to a third country or an international organization.

Condition 8

Assistance to the data controller

(a) The data processor shall promptly inform the data controller of any requests received from data subjects. The data processor may not respond to such requests itself unless authorized to do so by the data controller.

(b) The data processor shall assist the data controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the data processing. In performing its obligations under points (a) and (b), the data processor must comply with the instructions of the data controller.

(c) In addition to assisting the data controller as specified in point (b) of this section, the data processor must also assist the data controller in fulfilling the following obligations, considering the nature of the data processing and the information available to the data processor:

(1) The obligation to assess the impact of the planned data processing operations on the protection of personal data (hereinafter: Data Protection Impact Assessment), where a type of processing is likely to result in high risks to the rights and freedoms of natural persons;

(2) If the Data Protection Impact Assessment indicates that the processing is likely to result in high risks in the absence of measures taken by the data controller to mitigate the risk, the obligation to consult with the competent supervisory authority/authorities before proceeding with the processing

(3) The obligation to ensure the accuracy and currency of personal data, promptly notifying the data controller if the data processor becomes aware that the personal data it processes are inaccurate or outdated;

(4) The obligations set out in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall define in Annex III the appropriate technical and organizational measures that the data processor is required to take to assist the data controller in the application of this condition, as well as the scope and extent of such assistance.

Condition 9

Notification of data breach

In the event of a data breach, the data processor must cooperate with the data controller and assist the data controller in fulfilling its obligations under Articles 33 and 34 of Regulation (EU) 2016/679, taking into account the nature of the processing and the information available to the data processor.

9.1. Data breach involving data controlled by the data controller

In the event of a data breach involving personal data controlled by the data controller, the data processor shall assist the data controller as follows:

(a) Where applicable, promptly notify the relevant supervisory authority/authorities of the data breach after the data controller becomes aware of it (unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) Obtain the following information, which must be included in the notification to the data controller pursuant to Article 33(3) of Regulation (EU) 2016/679 and which must at least contain the following:

(1) The nature of the personal data involved, including – where possible – the categories and approximate number of data subjects and the categories and approximate number of data records concerned;

(2) The likely consequences of the data breach;

(3) The measures taken or proposed by the data controller to address the data breach, including, where appropriate, measures taken to mitigate any adverse effects resulting from the breach.

If it is not possible to provide all the information simultaneously, the initial notification must include the information available at that time, and any additional information must be provided without undue delay as it becomes available.

(c) Fulfilling the obligation under Article 34 of Regulation (EU) 2016/679 to notify the data subjects of the breach without undue delay (within 24 hours at the latest), if the data breach is likely to result in high risk to the rights and freedoms of natural persons.

9.2. Data breach involving data processed by the data processor

In the event of a data breach involving personal data processed by the data processor, the data processor shall notify the data controller without undue delay after becoming aware of the data breach. Such notification must include at least the following:

(a) A description of the nature of the data breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) Contact details for obtaining further information regarding the data breach;

(c) A description of the measures taken or proposed by the data processor to address the data breach, including, where appropriate, measures taken to mitigate any adverse effects resulting from the breach.

If it is not possible to provide all the information simultaneously, the initial notification must include the information available at that time, and any additional information must be provided without undue delay as it becomes available.

The Parties shall specify in Annex III all other elements that the data processor must provide when assisting the data controller in fulfilling its obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

CHAPTER III

CLOSING PROVISIONS

Condition 10

Non-compliance with the conditions and termination of the agreement

(a) Without prejudice to any provision of Regulation (EU) 2016/679, if the data processor breaches its obligations under these contractual conditions, the data controller may instruct the data processor to suspend the processing of personal data until the data processor complies with these conditions or the contract is terminated. The data processor must promptly inform the data controller if, for any reason, it is unable to comply with these conditions.

(b) The data controller is entitled to terminate the contract relating to the processing of personal data under these conditions if:

(1) The data controller has suspended the data processing by the data processor under point (a), and if compliance with these conditions is not restored within a reasonable period, but no later than one month after the suspension;

(2) The data processor has committed a serious or persistent breach of these conditions or its obligations under Regulation (EU) 2016/679;

(3) The data processor fails to comply with a binding decision of a competent court or supervisory authority concerning these conditions or obligations under Regulation (EU) 2016/679.

(c) The data processor is entitled to terminate the contract relating to the processing of personal data under these conditions if the data controller, after being informed by the data processor that its instructions violate legal requirements under point 7.1(b), insists on the instructions being followed.

(d) Following the evaluation session, the data processor will delete all personal data processed on behalf of the data controller. The anonymized (data that does not allow for personal identification) data will be stored for six months for model refinement purposes.

Dated: Budapest, 19th of February 2026

ANNEX I

List of Parties

Data controller [*name and contact information of the data controller and – if applicable – the name and the contact details of the data protection officer*]

Name: _____

Address: _____

Contact person

Name: _____

Position: _____

Phone no.: _____

E-mail: _____

Date:

_____

Signature

Data processor

Name: Ceph Assistant Korlátolt Felelősségű Társaság

Address: 1023 Budapest, Mecset utca 8. 2. em. 1. ajtó

Contact person

Name: Bendegúz H. Zováthi

Position: Co-Founder of Ceph Assistant

Phone no.: +36702842985

E-mail: bendeguz.zovathi@cephassistant.com

Date: 17/02/2026

ANNEX II

I. Name of the data processing:

Interface and functions for digital dental record analysis

Purpose of Processing Personal Data on Behalf of the Data Controller:

The data controller follows these steps to evaluate the digital dental record:

1. Upload the digital dental record and optionally provide related data (e.g., patient ID, treatment stage, gender, date of birth, missing teeth).

2. The program automatically places measurement points, calculates distances, angles and ratios interactively based on the selected analysis type, and displays comments and visualizations according to the measurements.

3. The data controller reviews and, if necessary, modifies the points and associated comments. Additionally, the data controller may write additional comments and a summary based on observations.

4. The data controller generates a report with their own provided data, the data of the person depicted in the uploaded image, and the analysis result table. The report may optionally include the evaluated image, the evaluation landmarks, and other visual representations of the values. The generated report is downloaded from the program and stored locally on the data controller's computer.

1. Categories of data subjects whose personal data are processed

Individuals whose data is uploaded by the data controller.

2. Categories of personal data processed

Mandatory: Digital dental record (defined by the upload interface, for example: cephalometric X-ray image, frontal or lateral photo image, 3D face scan, 3D intraoral scan).

Optional: Patient identifier, treatment stage, gender and date of birth, missing teeth

Links generated by the data processor do not automatically contain optional data. The data controller is responsible for any optional data entered.

3. Nature of data processing

Automated digital processing, analysis, report generation, storage, use of data in an anonymized manner (e.g., for training AI models), and deletion.

4. Duration of data processing

Until the report is completed or interrupted. Analysis interfaces may be reloaded within 24 hours.

Subject to a separate written agreement, analysis interfaces may be made publicly accessible via links and may remain valid for up to 2 years, and reports are available for 4 hours after generation. In this case, the Customer acknowledges that the link is public and therefore

shareable. Both the Service Provider and the Customer guarantee that they will not share the link with third parties (except for the customer concerned).

The uploaded image and the landmark coordinates will be stored anonymously in the data processor's database indefinitely.

ANNEX III

Technical and organizational measures ensuring data security

1) M*easures for pseudonymization and encryption of personal data:*

During the process, image data and patient identifiers are stored in separate databases to enhance privacy.

2) *Measures ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems and services:*

The confidentiality of data is ensured by user email addresses and passwords, its integrity is protected by system intrusion prevention, and availability is ensured until the end of the session by the high SLA level of the processor's sub-processors.

3) *Measures to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident:*

Analytical sessions are time-limited, allowing the process to be restored via a link that is valid for 24 hours, with the possibility of extending this duration to up to 2 years for certain partner-specific custom agreements.

In case the user accidentally clicks out or exits the session, the system prompts a confirmation to ensure the interruption was not intentional.

Continuous automatic monitoring of the server and immediate automatic restart in case of failure ensures constant availability of the service.

4) *Measures for user identification and authentication:*

Users can log in with a user ID (email address) and password, confirmed via email during registration. Previous analysis data is deleted, so the logged-in user cannot see previous analyses.

5) *Measures to protect data during transmission:*

Communication between parties is conducted over an encrypted channel.

6) *Measures to ensure the physical security of locations where personal data is processed:*

The processing location for personal data is provided by Microsoft Azure (sub-processor), which implements appropriate physical security measures. Beyond logical protection, the processor does not require higher physical security measures due to the low-risk level.

7) *Measures for internal IT and IT security management:*

The processor regulates IT security through internal procedures.

8) *Measure to ensure data minimisation*

The system is designed to ensure the input of only necessary data.

9) *Measure to ensure limited data retention*

Personal data entered is deleted at the end of the session.

10) *Measures to ensure accountability*

The processor documents its procedures and system events.

11) *Measures to ensure data deletion*

The processor uses technology that ensures irreversible deletion of data.

ANNEX IV

List of additional data processors

Microsoft Corporation, Azure Cloud Services (One Microsoft Way, Redmond, WA 98052, USA)