Personal Data Processing Agreement

entered into pursuant to Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council 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) (the "GDPR")

Parties

Doctor/Clinic – defined in the general terms and conditions (hereinafter the "**Controller**")

and

Estheticon, s.r.o., with its registered office at Dr. Milady Horákové 513/23a, Liberec IV-Perštýn, registered in the Regional Court for Ústí nad Labem, Section C, Entry 14604 (hereinafter the "**Processor**")

(the Controller and Processor also hereinafter the "**Parties**")

on the below-stated day, month and year enter into the following personal data processing agreement (hereinafter the "**Agreement**").

1. Subject and Purpose of the Agreement

1.1. The Controller and Processor work together under another contractual relationship involving communications, in particular offering the Controller's services to patients and enabling the transmission of partial content from the website www.estheticon.com using a widget. This cooperation involves, or can involve, the handover of personal data, where the Controller determines the purpose of the processing and provides the funds for the processing, and the Processor also processes personal data for the Controller within the confines of this Personal Data Processing Agreement.

1.2. This Agreement defines the rights and obligations of the Parties in the above-mentioned processing of personal data.

2. Personal Data Processing

2.1. The Processor is entitled to process the following personal data for the Controller:

First and last name

Phone number

Email

Procedure the potential patient is interested in

Text description of the problem

Photograph(s) attached to the message

Proposed date and time for consultation

IP address

Post – review of a doctor or discussion forum question answered by the doctor

(hereinafter the "Personal Data").

2.2. The Processor processes personal data only for the purposes of enabling potential clients (patients) to communicate with the Controller and enabling sharing of web content concerning the doctor using the widget.

2.3. The Controller is entitled to expand the purpose of processing in accordance with the law, where the instructions on additional processing must be given to the Processor in written form. For the purposes of this Agreement, written form includes email communication by the Parties addressed to the authorized persons.

3. Rights and Obligations of the Parties

3.1. The Processor undertakes to take technical, organizational and other measures to restrict unauthorized or random access, changes, destruction, loss or other unauthorized handling of or to the Personal Data. The Processor undertakes in particular as follows:

a) to use secure access to the PC only known to the Processor;

b) to use secure access to the database containing personal data, and the Processor must not display, save or disclose access information to a third party;

c) to perform the processing using software and services that meet the standard data security requirements and the standards set by the European Union;

d) not to make copies of the database without the prior consent of the Controller;

e) to use appropriate means of security, such as encryption or other appropriate and necessary means, always depending on the specific action and data;

f) not to allow access to third party data, unless said access is approved in writing by the Controller or is implied in this Agreement;

g) to maintain confidentiality regarding data.

3.2. The Processor also undertakes as follows:

a) to process the Personal Data only in the form as it was received from the Controller;

b) to process only the Personal Data for the purposes defined in this Agreement and only in the scope necessary to achieve said purposes;

c) not to combine Personal Data acquired for differing purposes;

d) to store the Personal Data only for the period stated in the duty to inform or in the end user's consent.

3.3. The Processor must archive on the Controller's behalf any and all personal data processing consents handed over to the Processor by end users. The Processor must surrender the consents to the Controller within two business days of the Controller's notice to do so.

3.4. The Processor must ensure that employees and other persons authorized by the Processor to process the Personal Data do so only in the scope and for the purposes pursuant to this Agreement and the GDPR.

3.5. The Processor and Controller undertake to process the Personal Data pursuant to this Agreement upholding the obligations stipulated in the GDPR and other generally binding legal regulations relating to this activity.

3.6. The Processor undertakes to correct, update, delete or relocate the Personal Data at the Controller's request without undue delay.

3.7. In the event that the data subject makes an objection pursuant to Article 21(1) of the GDPR to the Processor and it is found legitimate, the Processor undertakes to remove the defective situation immediately upon receiving the written notice from the Controller. Email communication from the Parties is also considered written communication.

3.8. The Processor must proceed with due professional care, follow the Controller's instructions and act and in accordance with the Controller's interests when performing under this Agreement. If the Processor discovers that the Controller is in breach of its obligations imposed by the GDPR, the Processor must inform the Controller of such fact immediately.

3.9. The Processor undertakes to provide the Controller with any and all information necessary to prove that the obligations stipulated in this Agreement or the GDPR concerning personal data have been met, and to enable the Controller or a third party bound by confidentiality toward the Controller to perform an audit in the appropriate scope. The audit must be announced with sufficient advance notice, at least 30 days before the audit takes place, and must not unreasonably infringe on the activities of the Processor. The Controller bears the costs of the audit not incurred by clear breach of obligations on the part of the Processor.

3.10. The Controller agrees that the Processor is entitled to entrust the processing of personal data to another processor without further specific permission from the Controller (hereinafter the "**Subprocessor**").

a) The Processor informs the Controller of any and all Subprocessors to whom it intends to entrust the processing of personal data, giving the Controller the opportunity to object to engaging such Subprocessors. This notice may be made in the form of a mass email

or through other electronic means. If the Controller does not make its objection to the Subprocessors within three business days, the Processor is entitled to engage said Subprocessor.

b) If the Controller objects to engaging the Subprocessor pursuant to point a) above, the Processor is entitled to give a termination notice on the provision of the services that require processing personal data, with a notice period of 14 days beginning on the day after the Controller receives the Processor's termination notice. The Processor may give the termination notice by email or other electronic means.

c) If the Processor engages the Subprocessor to perform certain processing activities, the Subprocessor must be bound by the same contractual obligations regarding personal data protection as those set forth in this Agreement and the GDPR. If the Subprocessor does not perform its obligations regarding data protection, the Processor is liable to the Controller for the performance of obligations on the part of that Subprocessor.

3.11. As of the date of entering into this Agreement, the Processor uses the following Subprocessors:

AWS Amazon Web Service (web hosting)

MaxMind, Inc.(determining position by IP address)

Google as part of Google Analytics (visitor statistics)

4. Duration of the Agreement

4.1. This Agreement is in effect for as long as the contractual relationship set forth in Article 1.1. of the Agreement is in effect.

4.2. In the event of any termination of this Agreement or termination of the processing of the Personal Data, the Processor must immediately destroy the Personal Data provided to the Processor on the basis of this Agreement, unless continuing to store them temporarily is in the legitimate and reasonable interest of the Processor.

5. Confidentiality

5.1. The Processor undertakes to maintain confidentiality regarding the Personal Data being processed, in particular not to make public, disseminate or disclose to persons other than an employee of the Processor or other authorized person authorized to process the Personal Data. The Processor must ensure that its employees and other authorized persons also adhere to the duty of confidentiality pursuant to Article 5 of the Agreement. This obligation on the part of the Processor shall remain in force even after the termination of this contractual relationship.

5.2. The Processor is further obliged to maintain confidentiality regarding the security measures taken to protect the personal data, even after this contractual relationship has been terminated.

6. Liability

6.1. If the Processor breaches its obligations established under this Agreement or the GDPR, the Processor is liable for any and all damage incurred due to said breach. The scope of the obligations also applies to damage caused to third parties and sanctions imposed by public authorities due to a breach of the GDPR or other regulation on Personal Data protection.

6.2. The Processor is also liable for damage caused by breach of this Agreement on the part of the Processor's employees.

7. Final Provisions

7.1. The invalidity or incomprehensibility of any provision of this Agreement has no effect on the validity of the other provisions of this Agreement.

7.2. The Parties undertake to provide each other with any and all necessary collaboration and materials for securing smooth, efficient implementation of this Agreement, in particular in the event of negotiations with the Personal Data Protection Office or other public authorities.