Data Processing Agreement

Appendix No. 2 to the Terms of Service for the Provision of Services by Electronic Means

In force from 2 November 2026 (previous wording from 18 September 2026). List of Sub-processors updated on 2 November 2026.

§ 1.

Definitions

1. **Processor** – the Service Provider within the meaning given to that term in the Terms.
2. **Controller** – the Salon, within the meaning given to that term in the Terms.
3. **Data** – personal data entrusted to the Processor for processing by the Controller in connection with the Principal Agreement.
4. **Sub-processor** – a further processor whose services the Processor uses in connection with the performance of the Principal Agreement.
5. **Terms** – the Terms of Service for the Provision of Services by Electronic Means, available on the Website (dotty.pl), i.e. the terms of the service under which the Processor makes available to the Salon the Application used to manage a beauty salon, together with the part of the Application intended for Salon Clients.
6. **GDPR** – 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).
7. **Principal Agreement** – the agreement concluded under the Terms, on the basis of which the Service Provider provides the Service to the Salon.
8. **DPA** – this agreement for entrusting the processing of personal data, constituting Appendix No. 2 to the Terms.

§ 2.

Introductory provisions

1. In connection with the conclusion by the Parties of the Principal Agreement, the Parties conclude an agreement for entrusting the processing of the Data.
2. The Controller entrusts for processing the Data in respect of which it acts as controller of personal data within the meaning of the GDPR, and the Processor undertakes to process them within the limits set out in the DPA and in generally applicable provisions of law.
3. Any processing of the Data by the Processor takes place solely on the documented instructions of the Controller, contained in particular in the Principal Agreement and also expressed by ordering further services, unless the Processor is required to process them by Union or Member State law to which the Processor is subject; in such a case the Processor informs the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest (Article 28(3)(a) of the GDPR).

4. The Data are processed for the purpose of performing the Principal Agreement and to the extent necessary for its proper performance.

5. This DPA supersedes all prior agreements, arrangements and understandings in this respect.

6. The Controller represents and warrants that it has legal bases for processing the Data and that entrusting the Data to the Processor for processing will not infringe the rights and freedoms of the data subjects or the provisions of law (in particular the GDPR).

7. The Data will be made available to the Processor solely for the purpose of performing the Principal Agreement.

8. The Controller will inform the Processor of any actions of the competent public administration authorities relating to the processing of the Data by the Controller.

9. The Processor takes all measures required by the applicable provisions of law, in particular by Article 32 of the GDPR, under which the Processor implements appropriate technical and organisational measures, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to ensure a level of security appropriate to that risk. In particular, the Processor applies the following technical and organisational measures: encryption (of transmission and of data), access control, pseudonymisation, backups and the ability to restore after an incident, regular testing of security measures, separation of roles; access to the data is granted only to authorised persons, to the extent necessary to operate the service, and passwords and access tokens are stored in encrypted form. Data concerning health are encrypted at the level of database columns, and photographs at the application level; the repository of backups stored outside the production infrastructure is encrypted. The frequency of backups, their retention period and the maximum acceptable extent of data loss are set out in the Terms.

10. The Data will be processed during the term of the Principal Agreement.

11. By concluding the DPA, the Controller instructs the Processor, as well as any person acting under the authority of the Processor who has access to the Data, to process the Data, which constitutes a documented instruction within the meaning of Article 28(3)(a) in conjunction with Article 29 of the GDPR.

§ 3.

Data

1. The Processor may process the Data entrusted to it for processing by the Controller for the purpose of performing the Principal Agreement and to the extent necessary for that purpose, for the term of the Principal Agreement. The retention period of the Data, including treatment records and Analysis results, is determined by the Controller. The Processor does not delete the Data on its own initiative and does not apply automatic deletion, unless the Controller enables such a function in the Application settings and specifies the period of its application. The Processor makes available to the Controller tools enabling the review of the Data and their deletion, including the deletion of the Data of an individual data subject and of a group of such persons. The obligation to determine the retention period of the Data and to delete Data that are no longer needed rests with the Controller.

2. The categories of persons whose personal data may be processed within the Application and whose processing is therefore entrusted to the Processor are defined as follows: Salon Clients, Salon Staff.

3. The types of Data entrusted include the data entered into the Application by the Salon, in particular identification and contact data (first name, surname, telephone number, e-mail address); age range; data on appointments and treatments; the content and history of consents given and withdrawn, together with signatures; data concerning health (consultation questionnaire, Analysis results, contraindications, allergies, medicines taken, skin condition) and photographs of the skin, which may include the image of the Salon Client – constituting special categories of personal data within the meaning of Article 9(1) of the GDPR.

4. The processing of the entrusted Data comprises the following processing operations: collection, recording, organisation, structuring, storage, retrieval, consultation, use, disclosure by transmission, alignment or combination, restriction, erasure or destruction.

§ 4.

Assistance and audits

1. Taking into account the nature of the processing, the Processor will provide assistance to the Controller (the "**Assistance**"). As part of the Assistance, the Processor will, insofar as this is possible, help the Controller by appropriate technical and organisational measures to fulfil its obligation to respond to requests from data subjects for the exercise of their rights laid down in Chapter III of the GDPR – where those obligations rest with the Controller in a given case – and will help the Controller to fulfil the obligations incumbent on the Controller under Articles 32 to 36 of the GDPR, taking into account the information available to the Processor.

2. As part of the Assistance, the Processor makes available to the Controller in the Application tools enabling it to handle data subjects' requests itself, in particular the export of the Data in a commonly used, machine-readable format, the permanent deletion of the Data together with treatment records and photographs, and the anonymisation of a client record while retaining the entries necessary for settlements.

3. The Processor is obliged to make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and to allow for and contribute to audits, including inspections (the "**Audit**"), conducted by the Controller or by an auditor mandated by the Controller.

4. If, in the Processor's opinion, instructions issued by the Controller infringe the GDPR or other provisions of Union law or Polish law, the Processor will immediately inform the Controller thereof.

5. The Processor may refuse to provide the Controller with information covered by secrecy protected by law, including the business secrets of the Processor or of third parties, as well as information constituting personal data other than the Data, if such information can be replaced by other information (including statements of the Processor); where this is not possible, such information will be made available to the Controller (or to persons designated by it) only at the Processor's registered office, after the Controller and all persons acting on behalf of the Controller have first concluded an agreement presented by the Processor obliging them to protect that information properly.

6. An Audit may be carried out after the Controller has first notified the Processor in writing of its intention to carry it out at least 14 days in advance, indicating the list of persons involved

in carrying out the Audit on the Controller's side. The notification should also specify the duration and scope of the Audit.

7. Where an Audit is not directly related to actions of the competent public administration authorities directed at the Controller in connection with the processing of data, or to an established and documented breach in the processing of the Data by the Processor, the total duration of Audits conducted by the Controller may not exceed three days in a calendar year.

8. An Audit may be carried out only after the Controller and all persons acting on behalf of the Controller have first concluded an agreement presented by the Processor obliging them to protect properly all information obtained in connection with the Audit.

9. An Audit is carried out during the Processor's working hours and may not in any way disrupt or adversely affect the Processor's day-to-day business.

10. The Processor cooperates with the authorities competent for the protection of personal data in the performance of their tasks.

11. Unless a different time limit results from the provisions of law or from this DPA, the Processor will perform activities in connection with the DPA, including the provision of any information, without delay and no later than within 30 days of receipt of the relevant request.

12. The Processor ensures that each person acting under its authority who is authorised to process the Data has committed himself or herself, in written or documentary form, to confidentiality with respect to the Data and the means of securing them, or is under an appropriate statutory obligation of confidentiality (Article 28(3)(b) of the GDPR). The obligation of confidentiality continues after the authorisation ends. The Processor grants authorisations only to the extent necessary for the performance of the Principal Agreement and keeps a record of the persons authorised.

§ 5.

Sub-processor

1. The Processor uses the services of Sub-processors on the basis of the Controller's general authorisation referred to in Article 28(2) of the GDPR, expressed in paragraph 4 below, subject to the procedure set out in paragraphs 6 to 8.

2. The Processor will impose on each Sub-processor, in particular by means of a contract, the same data protection obligations as those arising from the DPA, in particular the obligation to provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing meets the requirements of the GDPR.

3. Where a Sub-processor fails to fulfil its obligations in respect of the Data, the Processor remains fully liable to the Controller for the performance of the Sub-processor's obligations.

4. The Controller consents to the Processor's use of the Sub-processors indicated in the annex to this DPA. An amendment of the annex does not constitute an amendment of the DPA, and the provisions of paragraphs 6 to 8 of this section apply to it accordingly.

5. The analysis module of the Application uses a language model made available by an external provider acting as a Sub-processor. Only data concerning skin condition, the consultation questionnaire and treatment parameters are transferred to the model provider; age is transferred only as a range. The Application does not attach to the content transferred the first name, surname, contact details or identifiers of the Salon Client or of the Salon, and the

link between the result and a specific person remains solely within the Application. Photographs are transferred without metadata (EXIF) and without a file name. Content entered by the Controller or its staff in descriptive fields is transferred in the wording given by the Controller; the Controller undertakes not to include in those fields any data identifying the Salon Client. The Processor ensures that the model provider does not use the content transferred to train or test models, and that it deletes input and output data within the period specified by the provider.

6. Entrusting the processing of the Data to Sub-processors not indicated in the annex requires prior notification of that fact to the Controller, in order to enable it to object. The notification is made no later than fourteen days before the Data are entrusted to the Sub-processor. An objection may be raised no later than seven days before the Data are entrusted to the Sub-processor. Notification of the Processor's intention to entrust may be made in particular in electronic form.

7. In the absence of an objection, the Controller is deemed to have consented to the use of the Sub-processor.

8. If the Controller raises an objection, the Processor may not entrust the data to the Sub-processor to which the objection relates. In such a case the Processor will be entitled to terminate the Principal Agreement with immediate effect, and the Controller will not be entitled to any compensation on that account.

9. Any transfer of data to a third country or an international organisation by the Processor, i.e. outside the EEA, may take place only on the documented instructions of the Controller or in order to fulfil a specific requirement under Union or Member State law to which the Processor is subject, and in accordance with Chapter V of the GDPR. Where such a requirement is imposed on it by Union or Member State law to which the Processor is subject, the Processor informs the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

10. Where the Processor intends to use the services of a Sub-processor to carry out specific processing activities (on behalf of the Controller) that involve a transfer of personal data within the meaning of Chapter V of the GDPR, the Controller agrees that those entities may ensure compliance with Chapter V of the GDPR by means of standard contractual clauses adopted by the Commission in accordance with Article 46(2) of the GDPR, or that such a transfer may take place to a country in respect of which the European Commission has adopted an adequacy decision in accordance with Article 45 of the GDPR. If the adequacy decision on which a given transfer is based is declared invalid, repealed or suspended, the Processor will without delay implement another mechanism provided for in Chapter V of the GDPR or cease transferring the Data to that country.

§ 6.

Data breach

1. The Processor is obliged to notify the Controller without undue delay, and in any event no later than 48 hours after becoming aware of it, of each occurrence or suspected occurrence of an information security incident relating to the Data entrusted to the Processor, and in particular one constituting a personal data breach. The notification contains at least the information referred to in Article 33(3) of the GDPR, to the extent available to the Processor; the Processor provides missing information in phases, without undue further delay.

2. The Processor's obligation referred to in paragraph 1 above does not and will not constitute, and will not be interpreted as, a confirmation by the Processor towards data subjects that a personal data breach has occurred.

§ 7.

Final provisions

1. The DPA terminates upon termination of the Principal Agreement.

2. After the end of the provision of services involving the processing of the Data on behalf of the Controller, in particular in the event of termination of this DPA or of the Principal Agreement, the Processor, at the Controller's choice:

    a) deletes the Data and all existing copies thereof, unless European Union law or generally applicable provisions of Polish law require the storage of the personal data;
    b) returns all the Data to the Controller and deletes all existing copies thereof, unless European Union law or generally applicable provisions of Polish law require the storage of the personal data. In the cases referred to in points a) and b), deletion of the Data covers backups upon the expiry of the retention period of those backups set out in the Terms. Until then, the Data remaining in backups are not used and are restored only where it is necessary to restore data after an incident. The same applies to the deletion of the Data of an individual Salon Client during the term of the DPA.

3. In the event of termination or expiry of the Principal Agreement, the Controller should communicate to the Processor the decision referred to in the preceding paragraph no later than within 30 days of the date on which the Principal Agreement ends. During that period the Processor stores the Data and enables the Controller to export them in accordance with the Terms. If no such decision is communicated within that period, the Controller is deemed to have instructed the Processor to delete the Data, and all consequences thereof are borne solely by the Controller.

4. In matters not regulated herein, including the amendment of the DPA, the provisions of the Principal Agreement apply.

5. The DPA is drawn up in Polish and English. The Polish version is published at https://dotty.pl/umowa-powierzenia/. In the event of any discrepancy between the language versions, the Polish version prevails. In this English version the Polish terms "ADO" (administrator danych osobowych), "Procesor" and "Kolejny przetwarzający" are rendered as "Controller", "Processor" and "Sub-processor".

Annex:

List of Sub-processors

The Controller consents to the Processor entrusting the Data to the following Sub-processors:

Sub-processor	**Role**	**Location / transfer basis**
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany	hosting and infrastructure of the Application, including the database, photographs and backups, including the repository of backups stored outside the production server	Germany (EEA)

Sub-processor	Role	Location / transfer basis
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland	outgoing mail relay (system messages); synchronisation of the appointment calendar (on the Salon's express instruction)	Ireland (EEA) – the entrustment does not require a basis under Chapter V of the GDPR. As regards onward entrustment to Google LLC (USA): Commission Implementing Decision (EU) 2023/1795 (EU–US Data Privacy Framework) and, to the extent not covered by that decision, standard contractual clauses (Commission Implementing Decision (EU) 2021/914)
Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Ireland	language model generating a cosmetological interpretation (data without identifiers – § 5(5))	Ireland (EEA); the content is processed on servers in the United States: standard contractual clauses (Commission Implementing Decision (EU) 2021/914) incorporated in the provider's Data Processing Addendum
LINK Mobility Poland sp. z o.o., ul. Toszecka 101, 44-100 Gliwice, KRS 0000350201 (SMSAPI service)	sending SMS reminders of appointments on the Salon's instructions	Poland (EEA)