Synpleo Data Processing Agreement

Version 1.0 · Effective date: 2026-12-01

This Data Processing Agreement (the "DPA") is concluded under Article 28 of Regulation (EU) 2016/679 (GDPR) and forms part of the Agreement between Synpleo Development SRL (the "Provider") and the Client, concluded by signing a Synpleo Order Form. The Client is the controller and the Provider is the processor of the data of the Client's customers and visitors. Terms not defined here have the meaning given in the Synpleo Terms of Service.

1. Data processed

Service	Data subjects	Data
Website	website visitors	data submitted through forms (name, email, phone, message), hashed IP address, technical anti-abuse data
AI Assistant	visitors using the chat	conversation messages, contact details left in the conversation
Booking	the Client's customers	name, email, phone, selected service, date and time, booking history
Memberships	the Client's members	name, email, membership, QR code, check-in history

The data of the Client's own representatives and account users is not covered by this DPA; the Provider processes it as controller (Terms of Service, Article 12.1).

2. Purpose and duration

2.1. The Provider processes the data only to provide the services and only on the Client's documented instructions, including with regard to transfers outside the European Economic Area, unless required otherwise by EU or Member State law; in that case, the Provider informs the Client before processing, unless that law prohibits it. The Agreement and the settings the Client makes in the platform constitute these instructions.

2.2. The Provider does not sell the data and does not use it for its own purposes, including training AI models.

2.3. Processing lasts for the term of the Agreement. After termination, the Client may export its data for 30 days. The Provider then deletes the data within 30 days, except data it must retain by law (for example, invoices).

3. Provider's obligations

The Provider shall:

- immediately inform the Client if, in its opinion, an instruction infringes the GDPR or other EU or Member State data protection law;
- ensure the confidentiality of persons with access to the data;

- apply appropriate security measures under Article 32 GDPR: separation of each client's data, encrypted connections (HTTPS), role-based access, anti-abuse protection, backups;
- notify the Client within 48 hours of becoming aware of a personal data breach, with the information the Client needs to meet its obligations under Articles 33 and 34 GDPR;
- assist the Client in ensuring compliance with Articles 32 to 36 GDPR (security of processing, breach notification, data protection impact assessments and prior consultation), taking into account the nature of the processing and the information available to the Provider;
- assist the Client in responding to data subject requests (access, rectification, erasure), to the extent the Client cannot handle them itself in the platform;
- make available all information necessary to demonstrate compliance with Article 28 GDPR, and allow for and contribute to audits, including inspections, conducted by the Client or an auditor mandated by it, as follows:
  - audits are carried out first by written questionnaire, with at least 30 days' notice;
  - an inspection may take place only if the questionnaire response is not sufficient to demonstrate compliance, after a personal data breach, or at the request of a supervisory authority;
  - inspections take place at most once per year (except after a breach or at an authority's request), during business hours, with at least 30 days' notice, under confidentiality, and at the Client's cost.

4. Client's obligations

The Client shall:

- have a legal basis for the data collected through the services;
- inform its visitors and customers through its own privacy policy, including about the use of the Synpleo platform and the AI assistant;
- not upload special categories of data (Article 9 GDPR) without the Provider's written consent.

5. Sub-processors

5.1. The Client gives a general authorisation for the Provider to use sub-processors in the categories listed on the Sub-processors page (https://synpleo.com/legal/subprocessors).

5.2. The Provider shall notify the Client by email at least 30 days before adding or replacing any sub-processor, or moving data to another country, stating the sub-processor's name, category and data location. The Client may object on reasonable data protection grounds within this period. If no solution is found, the Client may terminate the Agreement without penalty and receives a pro rata refund of amounts prepaid for the period after termination.

5.3. The Provider imposes on sub-processors data protection obligations at least equivalent to those in this DPA.

5.4. The named list of sub-processors is provided to the Client on written request. The list and the notices under Article 5.2 are confidential information within the meaning of Article 10 of the Terms of Service.

6. Data location

Data is hosted primarily in data centres in the European Union. Some sub-processors (such as AI services and content delivery) may process data outside the European Economic Area. In that case, the Provider ensures that the safeguards required by the GDPR are in place (an adequacy decision, including the EU-US Data Privacy Framework, or standard contractual clauses).

7. Liability and precedence

7.1. Liability under this DPA is subject to Article 9 of the Terms of Service.

7.2. On data protection matters, this DPA prevails over the Terms of Service.

7.3. This DPA is published in English and Romanian. In case of discrepancy, the English version prevails.