Data Processing Agreement – Fylux Digital Solutions

Last updated: 8 November 2026 · Version 2.0

1. Subject matter and parties

This Data Processing Agreement ("**Agreement**") implements Article 28 of Regulation (EU) 2016/679 (General Data Protection Regulation, "**GDPR**") and Portuguese Law no. 58/2019. It governs the processing of personal data carried out by Fylux Digital Solutions ("**Fylux**" or "**Processor**") on behalf of the client that engages its services ("**Client**" or "**Controller**").

This Agreement forms an integral part of the service contract between the parties, which consists of the accepted proposal, the Terms of Service and, where applicable, the Fylux Plan Terms ("**Contract**"). It takes effect on acceptance of the proposal and remains in force for as long as Fylux processes personal data on behalf of the Client.

The full identification of the parties is stated in the accepted proposal.

The Portuguese version of this Agreement is the reference version. This English version is provided for convenience; in the event of any discrepancy, the Portuguese version prevails.

2. Definitions

Terms used in this Agreement have the meaning given in Article 4 of the GDPR. In addition:

Term	Meaning
Assistant	An AI system configured by Fylux that answers, replies, books or routes contacts on behalf of the Client, by phone, WhatsApp, email, chat or form.
End customer	A person who contacts the Client and interacts with the Assistant.
Client Data	Personal data processed by Fylux on behalf of the Client under the Contract.
Sub-processor	An organisation Fylux uses to carry out processing activities on behalf of the Client.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Client Data.

3. Roles of the parties

The Client is the **controller**: it decides the purposes and essential means of processing its end customers' data. Fylux is the **processor**: it processes that data only to provide the contracted services.

Data that Fylux processes to manage its own relationship with the Client (representatives' contact details, invoicing, use of the client area) is not covered by this Agreement; Fylux is the controller of that data under its Privacy Policy.

4. Description of the processing

Element	Description
Nature	Receiving, transcribing, automated analysis, recording, organising, consulting, routing, storing and deleting communications and booking data.
Purposes	Answering and replying to end customers on behalf of the Client; creating, changing, confirming and cancelling bookings; routing requests to the Client; producing summaries and activity reports; maintaining, testing and improving the configuration of the Client's Assistant; keeping the service secure.
Data subjects	The Client's end customers and prospective customers; Client staff who use the service.
Categories of data	Name; phone number; email; content of messages and emails; voice recordings and call transcripts, where enabled; booking data (service, date, time, staff member, notes); technical identifiers (caller number, WhatsApp identifier, date and time); other data the end customer chooses to share.
Special categories	Not intended. The Assistant is configured not to ask for them. If the Client operates in areas where they may arise (for example, healthcare), the parties agree additional safeguards in writing before go-live.
Duration	For the term of the Contract and until the data is deleted or returned under section 13.

5. Client instructions

Fylux processes Client Data only on documented instructions from the Client. The Contract, this Agreement and the approved configuration of the Assistant are the initial instructions. Further instructions may be given in writing (including by email or through the client area) and, if they involve work outside the scope, may be quoted.

Fylux will immediately inform the Client if it considers that an instruction infringes the GDPR or other data protection law, and may suspend that instruction until it is confirmed or changed.

If the law requires Fylux to process data for another purpose, Fylux will inform the Client before processing, unless the law prohibits it.

6. Client obligations

The Client warrants that:

- It has a lawful basis for processing its end customers' data and for using the Assistant;
- It gives end customers the information required by Articles 13 and 14 of the GDPR in its privacy policy, including that it uses technology providers for customer service;

- It authorises and keeps active the notices prepared by Fylux informing end customers that they are speaking to an automated assistant and, where applicable, that the call is recorded;
- It does not instruct Fylux to process data unlawfully;
- It responds to data subject requests, with Fylux's assistance as described in section 10.

7. Confidentiality

Fylux ensures that everyone authorised to process Client Data is bound by a contractual or statutory duty of confidentiality, which continues after the relationship ends. Access is granted only to those who need it to provide the service.

8. Security measures

Fylux applies technical and organisational measures appropriate to the risk, under Article 32 of the GDPR, as described in **Annex I**. The measures may evolve, provided the level of protection does not decrease.

9. Sub-processors

The Client gives Fylux **general authorisation** to use the sub-processors listed in **Annex II** and others that become necessary, on the following conditions:

- Fylux notifies the Client by email at least **15 days** in advance of any new or replacement sub-processor;
- The Client may object in writing within that period on reasonable data protection grounds. The parties will seek a solution; if none is possible, the Client may terminate the affected service without penalty;
- Fylux imposes on each sub-processor, by contract, data protection obligations equivalent to those in this Agreement;
- Fylux remains liable to the Client for its sub-processors' compliance.

10. Assistance to the Client

Taking into account the nature of the processing, Fylux assists the Client with:

- **Data subject rights**: if Fylux receives a request from an end customer, it forwards it to the Client within 5 business days and does not respond directly unless instructed. Fylux provides the technical means for the Client to view, export, correct or delete a data subject's data;
- **Security and breaches**: under sections 8 and 11;
- **Impact assessments and prior consultations**: by providing the information reasonably needed about Fylux's processing when the Client has to carry out a data protection impact assessment (Article 35 GDPR) or consult the supervisory authority (Article 36).

Assistance requiring significant work outside the normal service may be quoted, unless it results from a breach by Fylux.

11. Data breaches

If it becomes aware of a data breach affecting Client Data, Fylux will:

1. Notify the Client without undue delay and in any event within **48 hours**;
2. Provide, as soon as available, a description of the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken or proposed;
3. Immediately take steps to contain the breach and mitigate its effects;
4. Cooperate with the Client so that it can meet its duty to notify the supervisory authority (72 hours) and, where necessary, the data subjects.

Notification of a breach is not in itself an admission of fault.

12. International transfers

Fylux prefers providers and hosting regions in the European Union. Where a sub-processor processes data outside the European Economic Area, Fylux ensures that the transfer is based on an adequacy decision of the European Commission (including the EU-US Data Privacy Framework, for certified organisations) or on Standard Contractual Clauses approved by the Commission, with supplementary measures where necessary. Annex II states the location of each sub-processor.

13. Retention, return and deletion

13.1 During the Contract

Unless the Client instructs otherwise:

Data	Retention period
Call recordings (where enabled)	90 days
Transcripts and conversation history	90 days
Booking data	While in the Client's calendar; Fylux keeps no separate copy beyond what the service requires
Technical and security logs	Up to 6 months
Monthly reports	Aggregated data, without identifying data subjects

The Client may request shorter periods or, with justification, longer ones.

13.2 At the end of the Contract

At the end of the Contract, and as chosen by the Client within 30 days of termination, Fylux returns the Client Data in a structured, commonly used format (for example, CSV or JSON) and/or deletes it. If no choice is made, the data is deleted within **60 days** of termination, including backups, which are deleted in the normal rotation cycle. Fylux confirms deletion in writing on request.

Fylux may keep data after that period only where required by law, and only for the period and purpose required.

14. Use of data to improve the assistants

Fylux may review conversations with the Client's Assistant to improve **that Assistant's configuration** (answers, routing rules, knowledge base), as part of the service.

Fylux does **not** use Client Data to train general AI models or to serve other clients, and configures AI model providers so that data sent to them is not used to train those models, wherever the provider allows it. Aggregated, anonymised operating statistics (for example, response times) may be used to improve the service in general.

15. Audits and information

Fylux makes available to the Client the information needed to demonstrate compliance with this Agreement, including, on request, an up-to-date description of the security measures and the list of sub-processors with their data protection commitments.

The Client may carry out, or appoint an independent auditor bound by confidentiality to carry out, one audit per year, with at least 30 days' notice, during business hours and without disrupting operations, at its own cost. Additional audits are possible after a data breach or where required by the supervisory authority.

16. Liability

Each party is liable for the damage it causes by breaching its obligations, under Article 82 of the GDPR. Between the parties, the limitations of liability in the Contract apply, to the extent permitted by law.

17. Final provisions

- In the event of a conflict on data protection matters, this Agreement prevails over the other Contract documents.
- Changes to this Agreement must be made in writing. Fylux may update it to reflect changes in the law, giving the Client 15 days' notice.
- This Agreement is governed by Portuguese law and the GDPR. The courts of the District of Lisbon have jurisdiction.

18. Annex I · Technical and organisational measures

Access control

- Access to Client Data limited to the team working on the project, on a least-privilege basis;
- Two-factor authentication on all internal and administrative accounts;
- Credentials for the Client's tools stored in an encrypted vault, with key rotation, and never shared over insecure channels;
- Periodic review of access and immediate removal when no longer needed;

- Audit logs of relevant actions.

Encryption and transmission

- TLS encryption in transit;
- Encryption at rest at hosting and database providers;
- Logical separation of each Client's data.

Availability and resilience

- Hosting with high-availability, redundant providers;
- Regular encrypted backups, with recovery tests;
- Continuous monitoring of the Assistants and automatic alerts.

Development and operations

- Testing before any change goes to production;
- Security updates applied as a priority;
- Test environments without real end-customer data, wherever possible;
- Data minimisation: the Assistant only asks for the data needed for the task.

Organisation

- Confidentiality commitments from everyone with access;
- Documented incident and data breach response procedure;
- Assessment of providers before engaging them.

19. Annex II · Sub-processors

Category	Provider	Purpose	Location
Hosting	Vercel Inc.	Hosting of the application and booking pages	Global network; preferred region EU
Database	Supabase Inc.	Storage of configurations, bookings and logs	EU
Email	Resend Inc.	Sending confirmations, reminders and notifications	USA (Standard Contractual Clauses / EU-US Framework)
Calendar	Google Ireland Ltd.	Google Calendar integration, where the Client uses it	EU, with transfers to the USA
WhatsApp	Meta Platforms Ireland Ltd.	Sending and receiving messages through the WhatsApp Business Platform	EU, with transfers to the USA
Telephony	Telephony and voice provider stated in the proposal	Numbers, call routing and call recording	Stated in the proposal

Category	Provider	Purpose	Location
AI models	Language, transcription and voice model providers stated in the proposal	Understanding requests, generating answers, transcribing and synthesising speech	Stated in the proposal; EU region wherever available

The exact list applicable to each Client, including the telephony and AI model providers used in its Assistant, is set out in the proposal and updated under section 9.