Usage Guidelines – Fylux Digital Solutions

Last updated: 8 November 2026 · Version 2.0

1. Purpose and scope

These Usage Guidelines set out the acceptable use rules for the fyluxds.com website, the client area, the booking pages and all services of Fylux Digital Solutions ("**Fylux**"), including AI assistants, websites and automations. They apply to clients, their staff and anyone who uses the services.

They form part of the contract with each client, together with the Terms of Service. Their purpose is to protect the end customers who speak to the assistants, our clients, Fylux and the providers we rely on.

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

2. Principles for responsible assistants

Fylux assistants speak to real people on behalf of a business. For that reason, every assistant follows these principles, which the client cannot switch off:

- **Transparency**: the assistant identifies itself as an automated assistant at the start of the interaction or whenever asked, in line with Article 50 of Regulation (EU) 2024/1689 (the Artificial Intelligence Act);
- **Handover to a person**: the end customer must be able to reach a person at the business, by call transfer, a callback request or directions to another channel;
- **Honesty**: the assistant does not invent availability, prices, promotions or conditions the business has not approved, and says when it does not know;
- **Recording notice**: when calls are recorded or transcribed, the end customer is told at the start of the call;
- **Respect**: the assistant does not use manipulation, undue pressure or exploit the vulnerabilities of those who contact it.

3. Prohibited uses

It is prohibited to use Fylux's services, directly or indirectly, for:

3.1 Illegal or deceptive activities

- Any illegal activity, or promoting illegal products and services;
- Fraud, scams, phishing, identity theft or credential harvesting;
- Making the assistant impersonate a real person, a public body or another company;
- Misleading advertising or unfair commercial practices;
- Pyramid schemes, unlicensed gambling, or selling products that require authorisation without holding it.

3.2 Unsolicited communications

- Sending spam, by email, SMS or WhatsApp;
- Marketing calls or messages to people who have not consented or have objected, in breach of Portuguese Law no. 41/2004 and WhatsApp Business rules;
- Using purchased contact lists or lists obtained without a lawful basis;
- Mass automated calls (robocalls) or calls from hidden or spoofed numbers.

3.3 Unacceptable content

- Content that incites hatred, violence or discrimination;
- Harassment, threats, defamation or content that violates the privacy of others;
- Sexually explicit content, or any content involving or exploiting minors;
- Content that infringes copyright, trademarks or other intellectual property rights.

3.4 High-risk uses of AI

Fylux assistants may not be configured to:

- Give diagnoses or medical, legal, financial or other advice that requires professional qualifications;
- Make decisions with legal or similarly significant effects on people (for example, refusing credit, employment or access to essential services) without human involvement;
- Assess or classify people based on personal characteristics, behaviour or biometric data;
- Carry out any practice prohibited by Article 5 of the Artificial Intelligence Act.

Clients in sensitive sectors (healthcare, financial services, legal services) may use the assistants for administrative tasks, such as bookings and practical questions, under rules agreed in writing before go-live.

3.5 System security

- Accessing or attempting to access, without authorisation, the systems, accounts or data of Fylux, other clients or third parties;
- Testing for vulnerabilities without written authorisation (see section 8);
- Distributing malware, or using the services for denial-of-service attacks;
- Reverse engineering, decompiling or copying Fylux's tools;
- Circumventing technical or usage limits or security measures;
- Attempting to manipulate the assistants into revealing internal instructions, other clients' data or credentials (for example, through "prompt injection").

4. Client content and information

The client is responsible for the content and information it provides to Fylux to configure the assistants and the website (services, prices, text, images, answers). It must ensure that:

- The information is true and up to date;
- It holds the necessary rights to text, images, brands and other materials;
- The content complies with the law and with these Guidelines.

Fylux may refuse or remove content that breaches these rules, notifying the client.

5. Personal data

When using the assistants, the client processes its end customers' personal data and is responsible for that processing. In particular, it must:

- Have a privacy policy that mentions customer service through technology providers;
- Ask the assistant to collect only the data needed;
- Not instruct the assistant to collect special categories of data without safeguards agreed in writing;
- Respond to data subject requests, with Fylux's support.

The full rules are in the Data Processing Agreement.

6. Accounts, credentials and client area

- Each client-area user must have their own account; do not share credentials;
- Use strong passwords and enable two-factor authentication when available;
- The client is responsible for actions taken with its credentials and for removing access for staff who leave;
- If you suspect unauthorised access, tell Fylux immediately at hello@fyluxds.com;
- When giving Fylux credentials for your tools, do so through the client area or another secure channel indicated by Fylux, never in a plain message.

7. Fair use and technical limits

Plans include volumes set out in the proposal. The services may not be used in a way that compromises the stability of the infrastructure or harms other clients (for example, artificial traffic spikes or looping automations). If this happens, Fylux may temporarily limit or isolate resources, notifying the client, and propose a suitable plan.

8. Responsible vulnerability disclosure

If you find a security vulnerability in our services, contact us at hello@fyluxds.com with the subject "Security", describing the issue and how to reproduce it. We ask that you:

- Do not exploit the vulnerability beyond what is needed to demonstrate it;
- Do not access, alter or delete third-party data;
- Do not disclose the vulnerability publicly before we have had reasonable time to fix it.

We commit to replying within 5 business days, keeping you informed and not taking legal action against anyone who reports in good faith and follows these rules.

9. Fylux brand

Use of the Fylux brand, logo or materials requires prior written permission, except for factual references (for example, "website built by Fylux"). It is not permitted to suggest a partnership, sponsorship or affiliation without express permission. Websites built by Fylux may include a discreet reference to Fylux in the footer, which the client may ask to remove.

10. Conduct and communication

We expect respectful, professional communication between teams. We do not tolerate abuse, harassment, discrimination or threats, whether against the Fylux team or against end customers through the assistants.

11. Working together on projects

- Change requests follow the process agreed in the proposal, preferably through the client area;
- Urgent requests must be flagged as such and include the necessary information;
- Deliverables must be reviewed and approved within the agreed time frames;
- Out-of-scope changes are quoted before they start.

12. Payments

Subscriptions require timely payment. Non-payment may lead to suspension of the services, under the Terms of Service. Unfounded chargebacks may lead to immediate termination.

13. Consequences of breach

Fylux responds in proportion to the seriousness of the situation:

Situation	Usual response
Minor or unintentional breach	Written warning and time to correct it
Repeated or uncorrected breach	Suspension of the affected service until corrected
Serious breach (illegal activity, security risk, harm to third parties, risk of channels being blocked by the provider)	Immediate suspension, without notice, and possible termination of the contract

Fylux may also report situations to the competent authorities where required by law. Suspension due to a client's breach does not give rise to a refund.

14. Third-party provider rules

Some channels are subject to their providers' rules, which the client must also follow, in particular the WhatsApp Business Platform policies (Meta), telecom operators' rules and AI model providers' usage policies. Breaching those rules may lead the provider to block the channel, for which Fylux is not liable.

15. Changes and contact

Fylux may update these Guidelines. Material changes are notified to clients by email at least 15 days in advance, except where they result from a legal obligation or urgent security need.

For questions about these Guidelines or to report abusive use: hello@fyluxds.com.