

Data-processing agreement

Version 1, 2026-09-30.

This is a translation. The Portuguese text prevails.

1. Parties and scope

This agreement is part of the service agreement between the business that uses our services (the **client**, controller) and **Repete, Lda.**, Rua Marquesa de Alorna 38, 3.º Esq., 1700-304 Lisboa, Portugal, NIPC and VAT PT518 751 570 (**we**, processor), for Agentic Commerce by BlueForestCore, Agentic Onboarding by BlueForestCore and the services that go with them. It sets out what Article 28 of the General Data Protection Regulation (Regulation (EU) 2016/679, GDPR) requires. On personal data, it prevails over the service agreement.

Contact: info@repete.pt.

2. What we process, and why

- **Subject and purpose:** running the AI assistant on the client's website and channels, and the lead, order, booking, quote and support flows that go with it, only to provide the service to the client.
- **Nature:** hosting, storage, answers by AI models, sending messages and preparing reports for the client.
- **Duration:** as long as the service agreement, plus the deletion period in section 9.
- **People:** the client's customers and website visitors who use the assistant, and the client's staff who use the service.
- **Data:** what people write in the chat and the answers; contact details they choose to give, such as a name, an email or a phone number; order, booking and quote details; technical data such as the IP address. The service needs no special categories of data, and the client does not ask people for them.

3. Our duties

- We process the data only on the client's documented instructions: the service agreement, this agreement and the client's settings. If EU or Portuguese law requires other processing, we tell the client before it starts, unless that law forbids it. We tell the client if we think an instruction breaks data protection law.
- Everyone at Repete, Lda. who can access the data is bound by confidentiality.
- We take the measures of Article 32 GDPR described in section 6.

- We help the client answer people who exercise their rights, and with security, breach notifications, impact assessments and prior consultations (Articles 32 to 36 GDPR).
- We never use the data to train AI models, never sell it and never use it for advertising.
- The assistant always says it is an AI (Article 50 of Regulation (EU) 2024/1689).

4. Sub-processors

The client gives general written authorisation for these sub-processors, each bound by data protection terms that protect the data at least as well as this agreement does:

- **Amazon Web Services:** hosting, storage and the assistant's AI models, in EU regions.
- **Google Workspace:** email, including the reports, lead notifications and other emails the service sends on the client's behalf, and the Google Sheets and Drive files the client shares with us.
- **Google:** web search (Google Custom Search, and Gemini with Google Search in the client's admin assistant) and address suggestions at checkout (Google Places), and turning a location the person shares into a place name (Google Geocoding), only where the client uses them.
- **Twilio:** WhatsApp and SMS messages, only where the client uses those channels.
- **Telegram:** our team's internal alerts and the client's admin assistant. Automatic alerts carry masked details; a lookup by our team, and that assistant, can show full details.

We tell the client at least 30 days before we add or replace one. The client can object on reasonable data protection grounds; if we cannot resolve the objection, the client can end the service concerned. We remain fully liable to the client for the work of our sub-processors.

5. Transfers outside the EU

Hosting, storage and the assistant's AI models are in the EU. Where a sub-processor may process data outside the EU (Google, Twilio, Telegram), the transfer rests on an adequacy decision, the EU standard contractual clauses or another safeguard of Chapter V GDPR.

6. Security

- Encrypted connections and encryption at rest.
- Hosting, storage and the assistant's AI models in EU regions.
- Access only for the people who need it, with their own accounts.
- Logs of access and changes, kept no longer than security needs.
- Backups that keep deleted data for up to 35 days, then drop it.

- A regular review of these measures.

7. Personal data breaches

We tell the client without undue delay, and within 48 hours at the latest, after we become aware of a breach that affects the client's data, with what we know, its likely effects and what we are doing about it.

8. Information and audits

We give the client the information needed to show that we keep this agreement. The client can audit us, itself or through an independent auditor bound by confidentiality, once a year and after a breach, with 30 days' notice and at its own cost.

9. End of the service

When the service ends, we delete the client's personal data within 30 days, or return it first if the client asks before the end, unless EU or Portuguese law requires us to keep it. Deleted data leaves the backups within a further 35 days.

10. Liability and law

Liability follows the service agreement. Portuguese law applies, and the courts of Lisbon have jurisdiction.

Repete, Lda. · NIPC 518 751 570 · VAT PT518751570 · Rua Marquesa de Alorna 38, 3.º Esq., 1700-304 Lisboa · info@repete.pt · +351 93 110 8888 (WhatsApp) · BlueForestCore is a brand of Repete, Lda.