Privacy Policy

Version 2026-03-03 · Effective 3 March 2026

1. Who we are and our role

1.1 Data controller. This Privacy Policy explains how Bluemarlin Ventures S.L. ("BlueMarlin", "we", "us") collects and uses personal data in connection with the website bluemarlinchat.com and the BlueMarlin platform (the "Platform"). Our details are:

Bluemarlin Ventures S.L.
Avenida de San Antón 37, 29018 Málaga, Spain
Tax ID (CIF/VAT): ESB27665173
Email: info@bluemarlinchat.com

1.2 Two roles, explained plainly. BlueMarlin is a business-to-business service. Businesses ("customers") use the Platform to exchange WhatsApp messages with their own contacts and to manage their own records. This means we act in two different roles under the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the Spanish Organic Law 3/2018 (LOPDGDD):

- We are the **controller** for the data we decide how to use: your account and sign-in data, billing data, data about visits to our website, technical and security data, and the messages you send to us. This Policy describes that processing in full.
- We are a **processor** for the data our customers store or exchange through the Platform: their contacts, their WhatsApp conversations, their records, files, notes and knowledge base. For that data the customer is the controller, and we act only on the customer's instructions under our Data Processing Agreement, published at bluemarlinchat.com/dpa.

1.3 If you are a customer of a business that uses BlueMarlin. If you have exchanged WhatsApp messages with a business that manages its conversations on BlueMarlin, or your details appear in that business's records, that business is the controller of your data. Its own privacy notice applies and it is the right place to send your questions and requests. We help it fulfil those requests as its processor (see Sections 12 and 13), and we forward any request you send to us.

2. Who this Policy covers

This Policy applies to:

- **Visitors** of bluemarlinchat.com and of the public pages we host (for example a shared view or a published page under /share or /p).
- **Users**: people who sign up for BlueMarlin, are invited to an organization (a "workspace") or use the Platform, its API or its MCP server on behalf of a customer.
- **End users and contacts of our customers**: people who send or receive WhatsApp messages through a customer's number, including website visitors who start a WhatsApp chat through a customer's chat widget, and people whose details a customer stores in its records.
- **Sandbox participants**: people who pair their own phone with our shared sandbox WhatsApp number to evaluate the Platform.
- **People who contact us** by email or through other channels.

3. Data we collect

3.1 Account data (we are controller). When you create an account or are invited to a workspace we collect your name, email address, profile picture (from Google if you sign in with Google), an optional phone number, the workspaces you belong to and your role in each, your session identifiers, and your preferences (language, interface settings). Sign-in works with Google or with a one-time code sent by email; we never hold a password for you. We also keep evidence of your acceptance of our Terms of Service, this Policy and the Data Processing Agreement: the timestamp (UTC), the IP address, the browser identification string and the version label you accepted.

3.2 Billing data (we are controller). When a workspace subscribes to a paid plan we hold the billing name and address, the VAT identification number, the references of the customer and subscription objects created at our payment provider (Stripe), and invoice metadata (plan, amount, status, dates). Card details are entered on Stripe's own pages and are never transmitted to or stored by us. Meta's WhatsApp conversation fees are billed by Meta to the customer directly and are outside our billing data.

3.3 Customer data processed on behalf of our customers (we are processor). Each Platform feature is a processing activity carried out for the customer, who decides what data enters the Platform. Depending on the features a customer uses, this includes:

- **Inbox**: WhatsApp messages sent and received on the customer's own number(s) through the WhatsApp Business Platform (Cloud API), including message content, media, delivery and read status, timestamps and phone numbers in international (E.164) format. Where a number is connected in "coexistence" mode and continues to be used in the WhatsApp Business app, Meta synchronises messages and, where offered, prior chat history into the Platform.
- **Campaigns**: recipient lists, template variables, delivery and read tracking, opt-out keyword detection, do-not-contact restrictions and frequency capping.
- **Workspace / CRM**: collections of records with custom fields (text, phone, email, files, location with map, booking/calendar, relations, formulas, pages), views, tags, notes, segments and audiences, CSV/Excel imports and sequences.
- **Files**: uploads and message media, stored in private object storage and served through short-lived, time-limited links. Only organization logos, user avatars and widget configuration are served from a public CDN host.
- **Pages and publications**: PDF documents generated from records, and public read-only share links (views and pages) that the customer may protect with a password or an expiry date, including CSV/XLSX exports of shared views.
- **Chat widget**: a script the customer embeds on its own website that opens a WhatsApp conversation (a wa.me link). The widget fetches its configuration from our CDN and reads the browser language. It sets no cookies and stores nothing about the visitor on our side until the visitor writes on WhatsApp.
- **AI agent (customer-facing)**: the customer's knowledge base (texts, question-and-answer pairs, uploaded documents, pages crawled from URLs the customer provides), the audience-specific data-access configuration, and the logs of AI conversations.
- **AI assistant for the team (internal)**: assistant threads, the per-organization memory the assistant keeps, saved procedures ("skills") that may run on a schedule, and the audit log of every tool action (who, what, when, result).
- **Voice notes**: incoming WhatsApp voice messages and their automatic transcripts.
- **Public API and webhooks**: API key metadata (keys are stored only as one-way hashes), request logs kept for 48 hours, and the payloads of outbound webhooks the customer configures.

- **MCP server and third-party AI clients**: the workspace grants, scopes and tokens a customer creates when connecting its own AI tools (for example Claude Code, Claude Desktop, Cursor or any MCP-capable client) at mcp.bluemarlinchat.com.
- **Integrations chosen by the customer**: Airtable base imports (credentials stored encrypted), Revolut Business bank synchronisation (transactions synced into a collection after the customer's OAuth consent, with periodic re-consent), and Google Maps address autocomplete (which runs in the browser directly against Google).
- **Shared sandbox number**: pairings between a participant's phone and a workspace (created by sending "join" followed by the workspace code), and the conversations exchanged on the sandbox number, which remain in that workspace's inbox.
- **Calendar and booking reminders**: scheduled WhatsApp reminders for bookings stored in records.

Records may contain any data the customer chooses to store (bookings, bank transactions, imported Airtable data) and may therefore concern people who are not users of the Platform, such as the counterparties of a bank transaction.

3.4 Technical data (we are controller). When you access the website or the Platform we automatically record your IP address, browser identification string and timestamps in request logs (kept 48 hours), error reports (kept 7 days) and security logs. Error reports are scrubbed of phone numbers and message bodies before they leave our infrastructure.

3.5 Communications (we are controller). If you write to info@bluemarlinchat.com or hello@bluemarlinchat.com, we keep your message, your address and our reply for as long as needed to handle the matter and to document it.

3.6 Data we do NOT collect. We do not use analytics or advertising trackers of any kind, on the website or in the Platform: no Google Analytics, no pixels, no ad networks, no third-party tracking cookies. We do not store card numbers or any payment card details. We do not store passwords. We do not sell, rent or trade personal data, and we do not profile anyone for advertising.

4. Purposes and legal bases

We process personal data only for the purposes below, each on the legal basis indicated under Article 6(1) GDPR.

4.1 Providing the service (Art. 6(1)(b), performance of a contract). Creating and authenticating your account, sending sign-in codes and invitations by email, operating the workspaces you belong to, delivering WhatsApp messages and campaigns, generating AI responses, embeddings and transcripts where the customer has enabled those features, running the API, webhooks and MCP server, and answering your support requests.

4.2 Billing (Art. 6(1)(b) and (c)). Managing trials, subscriptions and payments through Stripe, issuing invoices and keeping the accounting and tax records that Spanish commercial and tax law require us to hold.

4.3 Evidence of acceptance (Art. 6(1)(b) and (f)). Recording when, from where and which version of our documents you accepted, so that we can prove the contract was concluded and defend our rights if a dispute arises.

4.4 Security and abuse prevention (Art. 6(1)(f), legitimate interest). Maintaining request, error and security logs, verifying webhook signatures, rate limiting, sandbox caps and campaign throttling, and investigating incidents. Our legitimate interest is to keep the Platform and its data safe; the data involved is technical metadata kept for short periods.

4.5 Compliance with legal obligations (Art. 6(1)(c)). Responding to lawful requests from authorities, handling data-subject requests, notifying personal data breaches and retaining records where a law requires it.

4.6 Processing on behalf of our customers (customer's legal basis). For the customer data described in Section 3.3 we act as processor. The legal basis is determined by the customer as controller; we only follow its documented instructions under the Data Processing Agreement.

4.7 Consent. We do not rely on consent for any processing described in this Policy. Sandbox pairing, integrations and AI features are activated by an explicit action of the customer or participant and fall under Sections 4.1 and 4.6. Should we ever ask for your consent for a specific purpose, we will say so clearly, and you may withdraw it at any time.

5. Where your data is stored (data residency)

5.1 Application and database in Germany. The application servers and the primary database run on dedicated servers in a data centre in Germany (European Union), operated by an ISO/IEC 27001-certified European infrastructure provider. The provider's identity is available on request to info@bluemarlinchat.com.

5.2 Backups. The database is backed up daily. Backups are kept for 7 days on the server, protected by the server's access controls, and for 30 days in object storage located under EU jurisdiction, where they are encrypted at rest by the provider.

5.3 Files and media. Uploaded files, message media and generated documents are stored in object storage configured for EU jurisdiction (Cloudflare), encrypted at rest by the provider.

5.4 Cache and resilience buffer. A managed cache service hosted in Frankfurt, Germany (Upstash) holds workspace-membership cache data and, only during a database incident, a short-lived buffer of inbound WhatsApp webhooks. That buffer may transiently contain message content.

5.5 Error monitoring. Error reports are sent to Sentry with EU data residency (Germany). Phone numbers and message bodies are scrubbed before an event leaves our servers.

5.6 The rule. Customer data at rest stays in the European Union. Data leaves the EU only transiently, and only for the specific services named in Section 6: AI generation, embeddings and transcription (Anthropic, OpenAI), transactional email (Resend), payments (Stripe), WhatsApp delivery (Meta) and sign-in with Google. Section 8 covers the safeguards for those transfers.

6. Sub-processors

6.1 List. We use the following providers to operate the Platform. Each processes personal data only for the purpose stated, under a written agreement that imposes data-protection obligations at least equivalent to ours.

Provider	Purpose	Data	Location and transfer mechanism
European infrastructure provider (ISO/IEC 27001; identity on request)	Hosting of application, database and backups	All platform data	Germany (EU); no transfer
Cloudflare, Inc.	Object storage (EU jurisdiction), CDN, DNS, DDoS protection	Files, media, generated PDFs, public assets; HTTP metadata	EU storage; global edge network; US company — EU-US Data Privacy Framework and SCCs

Provider	Purpose	Data	Location and transfer mechanism
Upstash, Inc.	Managed cache	Identifiers, membership cache, transient webhook buffer	Frankfurt, Germany; US company — SCCs
Functional Software, Inc. (Sentry)	Error monitoring	Technical error reports, request metadata, IP address	EU region (Germany); US company — DPF and SCCs
Stripe, Inc. / Stripe Payments Europe Ltd	Payments, invoices, subscriptions	Billing contact, card data (never seen by us), invoices	Ireland/US — DPF and SCCs
Resend, Inc.	Transactional email (one-time codes, invitations, notifications)	Email address, name, email content	US — SCCs
Meta Platforms Ireland Ltd / Meta Platforms, Inc. / WhatsApp LLC	WhatsApp Business Platform (Cloud API)	Phone numbers, message content, media, delivery status, templates	Ireland/US — DPF and SCCs. Meta is also an independent controller for the WhatsApp service itself
Anthropic, PBC	Language-model responses for the AI agent and the team assistant	Message text, knowledge excerpts, conversation context, record content read by tools	US — DPF and SCCs; API terms exclude training on inputs
OpenAI, L.L.C. / OpenAI Ireland Ltd	Text embeddings for knowledge search; speech-to-text for voice notes	Text chunks of knowledge sources; audio of voice notes	US/Ireland — DPF and SCCs; API terms exclude training on inputs
Google Ireland Ltd / Google LLC	Sign-in with Google (OAuth); Maps address autocomplete (browser-side)	Email, name and avatar at sign-in; addresses typed for autocomplete	Ireland/US — DPF and SCCs

6.2 Services the customer chooses to connect. Airtable, Revolut Business, and any MCP client and the AI vendor behind it are services a customer connects to its workspace under its own agreements with those providers. They receive data because the customer instructs the Platform to send it. They are independent third parties, not our sub-processors, and this Policy does not govern their processing.

6.3 Changes. We will give notice of any new sub-processor, or of a change in the purpose or location of an existing one, at least 30 days before it starts processing personal data, by email to workspace administrators and on the bluemarlinchat.com/dpa page. Customers who object on reasonable data-protection grounds may terminate the affected service without penalty, as set out in the Data Processing Agreement.

7. AI features

7.1 What is sent to AI providers. When a customer enables AI features, Anthropic receives the text needed for the requested task: the incoming message, relevant excerpts of the customer's knowledge base, recent conversation context and, when the team assistant uses a tool that reads workspace data, the content of the records involved, which may include contact details such as names or phone numbers. OpenAI receives text chunks of knowledge sources to generate the vector embeddings used for retrieval, and the audio of incoming voice notes for transcription.

7.2 What is not sent. AI providers never receive billing data, sign-in credentials, API keys or data from any workspace other than the one the request belongs to. Each organization's knowledge base, conversations and assistant memory are isolated from every other organization's.

7.3 No training. Both providers process the data under API terms that exclude the use of inputs and outputs to train their models. We do not use customer data to train models either.

7.4 Customer-facing AI agent. The agent answers incoming WhatsApp messages using the knowledge base and the per-audience data access the customer configures, and escalates to a human when it cannot help. It can be switched off by the customer for the whole organization, for an audience, or for a single conversation.

7.5 Team assistant. The internal assistant is available only to the customer's staff inside the Platform and is never exposed to end users. It acts on the customer's own workspace data, only in response to a team member's request or a procedure the team has saved. Every tool call is recorded in an audit log with the actor, a summary of the inputs and the outcome, and destructive actions require an explicit confirmation before they run.

7.6 Automated decision-making. The Platform does not make decisions based solely on automated processing that produce legal effects on individuals or similarly significantly affect them within the meaning of Article 22 GDPR. The AI agent produces replies, not decisions about people; campaigns deliver messages to recipients defined by the customer; the customer keeps full control over both. A customer that builds such a decision on top of the Platform is responsible, as controller, for complying with Article 22.

8. International transfers

8.1 Where transfers occur. Customer data at rest remains in the European Union (Section 5). Transfers outside the EU/EEA are limited to the transient processing by the US-established sub-processors listed in Section 6, and to EU-established providers that belong to US groups.

8.2 Safeguards. For each such transfer we rely on:

- the European Commission's adequacy decision for the EU-US Data Privacy Framework (DPF), where the provider is certified under it; and, otherwise or in addition,
- the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, incorporated in our agreement with the provider, together with a transfer impact assessment and supplementary measures: encryption in transit, data minimisation (each provider receives only the data its task needs) and the use of pseudonymous identifiers wherever possible.

8.3 Verification and copies. You can verify a provider's DPF certification at dataprivacyframework.gov. A copy of the applicable transfer mechanism is available on request to info@bluemarlinchat.com.

9. Retention

We keep personal data only for as long as the purpose requires, or as long as a law requires us to keep it. The periods below apply.

Data	Retention
Account data	Duration of the account; deleted within 30 days after an account-deletion request
Customer data (records, conversations, files, knowledge base, AI logs)	Duration of the subscription; erased within 30 days after organization deletion or termination

Data	Retention
Data of suspended accounts (end of trial without subscription, failed payment after the 7-day grace period)	30 days, then deleted
Acceptance evidence	Duration of the account plus the limitation period applicable to contractual claims
Billing records and invoices	6 years (Spanish commercial and tax law)
API request logs	48 hours
Application event log	30 days
Error reports (error monitoring)	7 days
Assistant temporary uploads	7 days
Sync run ledger (Airtable, Revolut)	30 days
Sandbox pairing	72 hours after the last inbound message
Sessions	Until expiry or sign-out
Database backups	30 days rolling; data erased from the live system rolls off backups within a further 30 days

When an organization is deleted, access is removed immediately (members, API keys, widgets and published links stop working); content is erased within 30 days and rolls off backups within a further 30 days. After a retention period ends, data is permanently deleted or anonymised.

10. Cookies

10.1 The cookies we set. The website and the Platform use only cookies that are strictly necessary for the service or that store a preference you have set yourself:

- **Session cookie** — keeps you signed in; not readable by scripts and sent only over encrypted connections.
- **Workspace cookie** — remembers the workspace you last opened.
- **Language cookie** — your language preference; kept for about 13 months.
- **Interface cookie** — an interface layout preference.

10.2 No banner, and why. We do not use analytics, advertising or tracking cookies, and no third party sets cookies through our pages. Under Article 22.2 of the Spanish Information Society Services Act (LSSI) and Article 5(3) of Directive 2002/58/EC (ePrivacy), cookies that are strictly necessary to provide a service the user has requested, or that store a preference the user has expressly chosen, are exempt from the consent requirement. Because every cookie we set falls into one of those two categories, no consent banner is shown. You can delete these cookies at any time in your browser; deleting the authentication cookie signs you out.

10.3 Chat widget. The chat widget that customers embed on their own websites sets no cookies and stores nothing about the visitor on our side.

11. Security

We apply the following technical and organisational measures, and we keep them under review:

- **Encryption in transit**: TLS 1.2 or higher for all traffic, with HSTS. Incoming webhooks from Meta and Stripe are signature-verified; outbound webhooks are signed with a per-organization secret.
- **Tenant isolation**: organization-level filtering is enforced in every database query, and all identifiers are non-guessable random values.
- **Authentication**: Google OAuth and email one-time codes, so no passwords are stored; sessions in cookies that are not readable by scripts and travel only over encrypted connections; delegated authorisation with consent and scoped, revocable tokens for MCP clients; API keys stored only as one-way hashes; credentials of third-party integrations encrypted at rest.
- **Files**: private storage with time-limited links; public storage holds only logos, avatars and widget configuration.
- **Infrastructure access**: the database server sits on a private network; administrative access is key-based, limited to named administrators and granted only in time-limited windows; routine diagnostics use read-only access.
- **Logging discipline**: logs redact phone numbers and message bodies, error monitoring scrubs phone numbers, and every AI tool action is audited (who, what, when, result), with confirmation required for destructive actions.
- **Backups**: daily, stored in the EU (object-storage copies encrypted at rest by the provider); the restore procedure is documented and rehearsed.
- **Operations**: rate limiting and abuse controls (per-organization sandbox caps, campaign throttling), dependency updates, automatically verified deployments with rollback, and health checks.
- **Data minimisation**: no analytics trackers; AI providers receive only the text needed for the task and never billing data; nothing is used to train models.
- **Incident response**: we notify affected customers of a personal data breach without undue delay and no later than 48 hours after becoming aware of it, providing the information required by Article 33(3) GDPR as it becomes available.

12. Your rights

12.1 The rights. Under Articles 15 to 22 GDPR you may ask us for access to your personal data and a copy of it; rectification of inaccurate or incomplete data; erasure; restriction of processing; portability of the data you provided to us, in a structured, commonly used, machine-readable format; and you may object to processing based on our legitimate interests, on grounds relating to your particular situation. Where processing is based on consent, you may withdraw it at any time.

12.2 How to exercise them. Send your request to info@bluemarlinchat.com from the email address linked to your account. If we cannot identify you from the sender address, we will ask for the information reasonably needed to confirm your identity before acting. We reply within one month of receiving the request. Where a request is complex or we receive many requests, we may extend this period by up to two further months; if so, we will tell you within the first month and explain why. Requests are free of charge unless they are manifestly unfounded or excessive.

12.3 Data we hold as processor. If your request concerns data that a business stores or exchanges through BlueMarlin, that business is the controller (Section 1.3). We forward your request to it without undue delay and help it respond; we cannot act on such data on our own initiative.

12.4 Complaints. You have the right to lodge a complaint with a supervisory authority, in particular in the EU Member State of your habitual residence, place of work or place of the alleged infringement (Art. 77 GDPR). The authority for BlueMarlin is the Agencia Española de Protección de Datos (AEPD), C/ Jorge

Juan 6, 28001 Madrid, Spain, www.aepd.es. You are not required to contact us before the AEPD, although we welcome the chance to address your concern first.

13. How to delete your account and data

13.1 Users of BlueMarlin. To delete your account and all personal data associated with it, send an email to info@bluemarlinchat.com from the email address linked to your account, stating that you want your account and data deleted. We will confirm receipt and permanently delete your account data, the data of any workspace of which you are the sole owner, its files and conversations, within 30 days; backups containing that data roll off within a further 30 days. The only data we keep beyond that point are billing records and invoices, which Spanish tax law requires us to retain for 6 years, and the minimal record needed to document that the deletion was performed. Workspace owners can also delete an entire workspace from the workspace settings, with the same effect.

13.2 End users of businesses that use BlueMarlin. If you are a customer, lead or contact of a business that uses BlueMarlin (for example, you exchanged WhatsApp messages with a company that manages its conversations on our Platform, or you started a chat through its website widget), that business is the controller of your data. Please send your deletion request to that business; we will assist it in fulfilling the request as its data processor. You may also write to us at info@bluemarlinchat.com and we will forward your request to the business concerned and confirm to you that we have done so.

14. Children

The Platform is a business-to-business service for companies and the people authorised to act for them. It is not intended for anyone under 16 years of age, and we do not knowingly collect personal data from children. If we learn that we hold such data, we delete it promptly. Customers must not use the Platform to process children's data without a lawful basis.

15. Third-party links and services

The website and the Platform link to and connect with third-party services: WhatsApp itself, the Stripe billing portal, Google sign-in, and the services a customer chooses to connect such as Airtable, Revolut Business or an MCP client. Those services are governed by their own privacy notices, not by this Policy. In particular, Meta is an independent controller for the WhatsApp service, and its own terms and privacy policy apply to your use of WhatsApp.

16. Changes to this Policy

We may update this Policy to reflect changes in the Platform, our providers or the law. Each version carries a version label and an effective date at the top of the document. For material changes we give at least 30 days' notice before the new version takes effect, by email to account holders and through the Platform, and users are asked to accept the new version on their next sign-in. Corrections, clarifications and changes that only add safeguards for you may take effect immediately. Previous versions are available on request.

17. Contact

For any question about this Policy, to exercise your rights, or to request our Data Processing Agreement or the identity of our infrastructure provider:

Bluemarlin Ventures S.L.
Tax ID (CIF/VAT): ESB27665173
Avenida de San Antón 37
29018 Málaga, Spain
Email: info@bluemarlinchat.com
Support: hello@bluemarlinchat.com

This Policy is governed by Spanish law and by Regulation (EU) 2016/679. It is published in English; the English version prevails.