Data Processing Agreement

Version 2026-03-03 · Effective 3 March 2026

This Data Processing Agreement (the "DPA") forms part of the Terms of Service at https://bluemarlinchat.com/terms (the "Terms") and governs the processing of personal data by Bluemarlin Ventures S.L. on behalf of the customer under Article 28 of Regulation (EU) 2016/679 (the "GDPR"). The current version is published at https://bluemarlinchat.com/dpa (PDF at https://bluemarlinchat.com/dpa.pdf).

1. Parties and conclusion of this DPA

1.1 Parties. This DPA is entered into between (a) Bluemarlin Ventures S.L., a limited liability company under the laws of Spain, tax identification number ESB27665173, registered address Avenida de San Antón 37, 29018 Málaga, Spain (the "Processor"), and (b) the legal entity that holds an organization account (workspace) on the Services and on whose behalf the Terms have been accepted (the "Customer" or "Controller").

1.2 Incorporation. This DPA is incorporated by reference into the Terms and forms an integral part of the agreement between the parties for the Services (together, the "Agreement").

1.3 Electronic conclusion. This DPA is concluded in electronic form, as permitted by Article 28(9) GDPR, when a person authorised to bind the Customer accepts the Terms, the Privacy Policy and this DPA on the acceptance screen shown, which displays or links to the full text of each document, before first access to the Services. By accepting, that person represents that they have authority to bind the Customer.

1.4 Acceptance evidence. For each accepting user the Processor retains the timestamp of acceptance (UTC), the IP address, the browser user-agent string and the version label accepted. When a new version takes effect, users are asked to accept again and fresh evidence is recorded.

1.5 Countersigned copy. On request to info@bluemarlinchat.com the Processor will provide a countersigned PDF copy of this DPA identifying the Customer's organization and the version accepted.

1.6 Precedence. In the event of a conflict between this DPA and the Terms, this DPA prevails with respect to the processing of personal data.

2. Definitions

2.1 Terms defined in Article 4 GDPR ("controller", "processor", "data subject", "personal data", "personal data breach", "processing", "supervisory authority") have the meaning given there. References to Articles are to the GDPR unless stated otherwise.

2.2 "Applicable Data Protection Law" means the GDPR, Spanish Organic Law 3/2018 (LOPDGDD), any national law supplementing the GDPR that applies to the processing and, where the Customer is established there, the UK GDPR and Data Protection Act 2018 or the Swiss Federal Act on Data Protection (FADP).

2.3 "Customer Data" means all personal data that the Customer, its users, its contacts or its end customers submit to, generate in or cause to be collected by the Services and that the Processor processes on the Customer's behalf, as described in Annex I. It excludes Account Data (data of the Customer's users needed to operate their accounts), Billing Data and Technical Data (request logs, error reports, security logs), of which the Processor is a controller under the Privacy Policy at https://bluemarlinchat.com/privacy.

2.4 "Services" means the BlueMarlin platform at https://bluemarlinchat.com, including its web application, public API, outbound webhooks, MCP server, embeddable chat widget, shared sandbox WhatsApp number and related features provided under the Terms.

2.5 "Sub-processor" means any third party engaged by the Processor to process Customer Data on its behalf in providing the Services. "Data Residency Region" means the European Union. "SCCs" means the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914, as amended or replaced. "Business Day" means any day other than a Saturday, Sunday or public holiday in Málaga, Spain.

3. Roles and scope

3.1 Roles. As between the parties, the Customer is the controller of Customer Data and the Processor is its processor. Where the Customer acts as processor for a third-party controller, it warrants that it is authorised to give the instructions in this DPA and remains the Processor's sole point of contact.

3.2 Scope. This DPA applies to all processing of Customer Data in connection with the Services. The details of the processing are set out in Annex I.

3.3 Instructions. The Customer's complete documented instructions are (a) the Agreement, including this DPA; (b) the Customer's use of the features of the Services, including the configuration, integrations and connections it enables; and (c) any further written instructions agreed between the parties. Instructions outside the functionality of the Services require the Processor's prior written agreement and may be charged.

3.4 Infringing instructions. The Processor shall immediately inform the Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data-protection provisions, and may suspend its execution until the Customer confirms or amends it.

3.5 WhatsApp. Messages are transmitted through the WhatsApp Business Platform operated by Meta Platforms Ireland Ltd and its affiliates. Meta acts as a Sub-processor for the transmission of the Customer's messages and, separately, as an independent controller for the WhatsApp service used by the Customer's contacts, whose terms the Customer accepts directly with Meta when connecting its number.

3.6 No processing for own purposes. The Processor shall not process Customer Data for any purpose other than providing the Services on the Customer's instructions, shall not use it to train or improve machine-learning models and shall not sell or disclose it for its own commercial purposes. If the Processor determines the purposes and means of processing in breach of this DPA, it is considered a controller in respect of that processing (Article 28(10)).

4. Customer obligations

4.1 Lawfulness. The Customer is responsible for the lawfulness of the processing of Customer Data, including a valid legal basis under Article 6 (and, where relevant, Article 9) for each processing activity, for the accuracy and minimisation of Customer Data, and for its own obligations as controller, in

particular under Articles 5, 12 to 22, 24, 25, 30 and 33 to 35.

4.2 Information to data subjects. The Customer shall provide data subjects with the information required by Articles 13 and 14, including the use of WhatsApp as a channel, the use of automated replies generated by an AI agent where enabled, and the processing of their data by the Processor as its service provider.

4.3 Consent for WhatsApp messaging. The Customer shall obtain and be able to evidence each contact's prior opt-in to receive WhatsApp messages where required by Applicable Data Protection Law, Article 13 of Directive 2002/58/EC as implemented nationally, Spanish Law 34/2002 (LSSI) or the WhatsApp Business Messaging Policy, shall honour opt-outs and keep contact restrictions (do-not-contact) up to date, and shall not use the campaign feature for unsolicited communications.

4.4 Special categories. The Services are not designed for special categories of personal data (Article 9), data relating to criminal convictions (Article 10) or children's data. The Customer shall not submit such data unless it has a valid legal basis and has notified the Processor in writing at info@bluemarlinchat.com beforehand so that any additional measures can be agreed.

4.5 Appropriate configuration. The Customer is responsible for configuring the Services appropriately, in particular for (a) granting, reviewing and revoking user access rights and roles; (b) creating, protecting (password, expiry) and revoking public share links to views and pages; (c) the AI agent settings, including the audiences for which it is enabled, the data access granted per audience, the knowledge-base contents and switching the agent off for the organization, an audience or a conversation; (d) the third-party services and clients it connects (MCP clients and their AI vendors, Airtable, Revolut Business) and the scopes granted to them; (e) issuing, scoping and revoking API keys and securing its webhook endpoints; and (f) the content it publishes through the widget.

4.6 Users and sandbox. The Customer is responsible for the acts and omissions of its users. Where it uses the shared sandbox number, it shall pair only telephone numbers whose holders have agreed to take part in the evaluation and shall not use the sandbox for production communications.

5. Processor obligations

5.1 Documented instructions (Article 28(3)(a)). The Processor shall process Customer Data only on documented instructions from the Customer as described in clause 3.3, including with regard to transfers to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject; in that case the Processor shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

5.2 Confidentiality of personnel (Article 28(3)(b)). The Processor shall ensure that every person authorised to process Customer Data has committed to confidentiality in writing or is under an appropriate statutory obligation of confidentiality, and processes Customer Data only to the extent necessary for their role. Access by the Processor's personnel is restricted to named administrators and granted only when necessary to operate, support or secure the Services (Annex II).

5.3 Security (Article 28(3)(c)). The Processor shall implement and maintain the technical and organisational measures in Annex II, which the parties agree are appropriate under Article 32 having regard to the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing and the risks to data subjects. The Processor may update the measures provided the updates do not materially reduce the overall level of protection.

5.4 Sub-processors (Article 28(3)(d), 28(2) and 28(4)). The Processor shall engage Sub-processors only in accordance with clause 7, shall impose on each of them by written contract data-protection obligations providing a level of protection substantially equivalent to this DPA, and remains fully liable to the Customer for their performance.

5.5 Assistance with data-subject rights (Article 28(3)(e)). Taking into account the nature of the processing, the Processor shall assist the Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling its obligation to respond to requests for exercising data-subject rights under Chapter III. The Services allow the Customer to search, access, rectify, export, restrict and erase Customer Data relating to a data subject without the Processor's involvement; requests addressed directly to the Processor are forwarded to the Customer within five Business Days (clause 10).

5.6 Assistance with Articles 32 to 36 (Article 28(3)(f)). Taking into account the nature of the processing and the information available to it, the Processor shall assist the Customer in ensuring compliance with Articles 32 to 36 (security of processing, notification of personal data breaches to the supervisory authority and to data subjects, data protection impact assessments and prior consultation), through the information in this DPA and its Annexes, answers to reasonable written questions and, for a data protection impact assessment concerning the Customer's use of the Services, the further information reasonably available to it. Clause 9 governs personal data breaches.

5.7 Deletion and return (Article 28(3)(g)). At the Customer's choice, the Processor shall delete or return all Customer Data after the end of the provision of the Services and delete existing copies, unless Union or Member State law requires storage. Clause 12 sets out the procedure and timelines.

5.8 Information and audits (Article 28(3)(h)). The Processor shall make available to the Customer all information necessary to demonstrate compliance with Article 28 and this DPA, and shall allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer, in accordance with clause 11. The Processor shall immediately inform the Customer if an instruction infringes data-protection law (clause 3.4).

5.9 Records and cooperation. The Processor shall maintain the record required by Article 30(2), cooperate on request with the competent supervisory authority (Article 31) and maintain a data-protection contact at info@bluemarlinchat.com.

6. Data location and hosting

6.1 Commitment. Customer Data at rest is stored exclusively within the Data Residency Region (the European Union). The Processor shall not store Customer Data at rest outside the European Union except as set out in this clause and Annex III.

6.2 Storage locations. As at the effective date, Customer Data at rest is stored as follows:

Component	Content	Location
Application servers and primary database	All platform data: contacts, records, conversations, messages, notes, campaigns, knowledge base, AI logs and memory, configuration	Dedicated servers in a data centre in Germany (EU), operated by an ISO/IEC 27001-certified European infrastructure provider
Database backups	Daily backups of the primary database	Database server (7 days, protected by the server's access controls) and object storage under EU jurisdiction (30 days, encrypted at rest by the provider)

Component	Content	Location
Files, media and generated documents	Record files, message media, voice notes, campaign and template media, knowledge documents, generated PDFs	Object storage under EU jurisdiction (Cloudflare, EU jurisdiction setting), encrypted at rest by the provider
Public assets	Organization logos, user avatars, widget configuration	Public object storage under EU jurisdiction, served through a CDN host
Cache and resilience buffer	Organization and membership identifiers; during a database incident only, a short-lived buffer of inbound WhatsApp webhooks that may transiently contain message content	Managed cache service in Frankfurt, Germany (Upstash)
Error monitoring	Technical error reports and request metadata, phone numbers and message bodies scrubbed before transmission	Sentry, EU data residency (Germany)

6.3 Transient processing outside the EU. Customer Data leaves the European Union only transiently, in the course of a request, and only through the Sub-processors listed in Annex III for the purposes listed there: transmission of WhatsApp messages; generation of AI responses and the embeddings and voice-note transcriptions that support them; transactional email; payment processing; sign-in with Google; and the global edge network of the content-delivery and DDoS-protection provider through which HTTP requests are routed.

6.4 Relocation of primary storage. The Processor shall not move the primary storage of Customer Data (application servers, primary database, backups or file storage) outside the European Union without at least 30 days' prior written notice by email to the owner of the Customer's organization and by publication at https://bluemarlinchat.com/dpa. If the Customer objects on reasonable data-protection grounds within that period and no solution is found in good faith before the relocation takes effect, the Customer may terminate the Agreement without penalty and clause 12 applies.

6.5 Identity of the hosting provider. For security reasons the Processor does not name its infrastructure provider in public documents. The provider's legal name, the data-centre location and evidence of its ISO/IEC 27001 certification are disclosed on request to info@bluemarlinchat.com under the confidentiality obligations of the Agreement. Annex IV summarises this clause in a form the Customer may reproduce in its own vendor assessments.

7. Sub-processors

7.1 General authorisation. The Customer gives the Processor general written authorisation, within the meaning of Article 28(2), to engage the Sub-processors listed in Annex III for the services, data and locations described there, and further Sub-processors in accordance with this clause. The current list is published at https://bluemarlinchat.com/dpa.

7.2 Flow-down. The Processor shall conclude a written contract with each Sub-processor imposing data-protection obligations that provide a level of protection substantially equivalent to this DPA, in particular on confidentiality, security, assistance, deletion and transfers to third countries (Article 28(4)). On request the Processor shall provide a summary of those terms, redacting commercial and confidential information.

7.3 Notice of changes. The Processor shall inform the Customer of any intended addition or replacement of a Sub-processor at least 30 days before it starts processing Customer Data, by email to the owner of the Customer's organization and by updating the list at https://bluemarlinchat.com/dpa, identifying the Sub-processor, its service, the data concerned, the location of processing and the transfer mechanism.

Where a change is urgently required to preserve the security or availability of the Services, the Processor may shorten the notice period and shall inform the Customer without undue delay, stating the reasons.

7.4 Right to object. The Customer may object to an intended change on reasonable data-protection grounds by written notice to info@bluemarlinchat.com within the notice period, stating the grounds. The parties shall discuss the objection in good faith. If no solution is found within 30 days of the objection, the Customer may terminate the Service or feature affected by the change, or the Agreement as a whole where the change affects the core of the Services, without penalty and with a pro-rata refund of prepaid fees for the terminated Service, by written notice within a further 15 days. Failure to object within the notice period is deemed acceptance.

7.5 Liability. Where a Sub-processor fails to fulfil its data-protection obligations, the Processor remains fully liable to the Customer for the performance of that Sub-processor's obligations (Article 28(4)).

7.6 Not Sub-processors. Services the Customer chooses to connect (Airtable, Revolut Business, MCP-capable clients and the AI vendors those clients use) and the endpoints to which it directs webhooks are third parties engaged by the Customer under its own agreements. They are not Sub-processors, and the Customer is responsible for the transfer of Customer Data to them. The same applies to the Customer's use of the WhatsApp Business app on a number in coexistence mode.

8. International transfers

8.1 General. The Processor shall not transfer Customer Data to, or allow access from, a country outside the European Economic Area not covered by an adequacy decision of the European Commission except in accordance with Chapter V and this clause. Every such transfer to a Sub-processor is documented in Annex III with the mechanism relied on.

8.2 Adequacy decisions. Where a Sub-processor is established in a country covered by an adequacy decision, or is certified under the EU-U.S. Data Privacy Framework (Commission Implementing Decision (EU) 2023/1795), the Processor relies on that decision. Certification status can be verified at https://www.dataprivacyframework.gov.

8.3 Standard Contractual Clauses. Where no adequacy decision applies, or as a fallback should the decision relied on cease to apply, the Processor relies on the SCCs concluded with the Sub-processor (Module 3, processor to processor, or the module appropriate to the parties' roles), supported by a transfer impact assessment and supplementary measures: encryption of all data in transit (TLS 1.2 or higher), data minimisation so that each Sub-processor receives only the data necessary for its function, pseudonymous identifiers instead of directly identifying data where the function permits, and contractual commitments from AI Sub-processors that inputs are not used to train their models. The Processor shall reassess a transfer where the law or practice of the destination country materially changes, shall review public-authority requests for access to Customer Data and challenge them where there are grounds to do so, and shall inform the Customer unless legally prohibited.

8.4 United Kingdom and Switzerland. Where the Customer is established in the United Kingdom, transfers of Customer Data from the United Kingdom to third countries are covered by the International Data Transfer Addendum to the SCCs issued by the Information Commissioner. Where the Customer is established in Switzerland, the SCCs are read with the amendments required by the Federal Data Protection and Information Commissioner (references to the GDPR read as references to the FADP; the FDPIC as competent supervisory authority; data subjects in Switzerland may enforce their rights in Switzerland).

8.5 Customers outside the EEA. Where the Customer is itself established outside the European Economic Area, the United Kingdom, Switzerland or a country covered by an adequacy decision, the provision of the Services involves a transfer of Customer Data from the Processor in the European Union to the Customer. For that transfer the parties agree that Module 4 (transfer processor to controller) of the SCCs applies and is incorporated by reference, with the Processor as data exporter and the Customer as data importer; Annex I of this DPA serves as Annex I.B and Annex II of this DPA as Annex II of the SCCs; the optional docking clause does not apply; the governing law and courts are those of Spain. Where an adequacy decision subsequently covers the Customer's country, the parties may rely on it instead.

8.6 Changes in law. If a transfer mechanism relied on under this clause is invalidated, the parties shall cooperate in good faith to implement an alternative lawful mechanism without undue delay. Until then the Processor shall suspend the affected transfer to the extent technically possible without interrupting the Services, and the Customer may terminate the affected Service under clause 7.4 if the transfer cannot be made lawful.

9. Personal data breach

9.1 Notification. The Processor shall notify the Customer without undue delay, and in any event no later than 48 hours, after becoming aware of a personal data breach affecting Customer Data, by email to the owner of the Customer's organization and to any additional security contact the Customer has notified in writing to info@bluemarlinchat.com.

9.2 Content. To the extent the information is available, the notification shall (a) describe the nature of the breach, including where possible the categories and approximate number of data subjects and of personal data records concerned; (b) give the name and contact details of the Processor's contact point; (c) describe the likely consequences of the breach; and (d) describe the measures taken or proposed to address it and, where appropriate, to mitigate its possible adverse effects. Where it is not possible to provide all of this information at once, the Processor shall provide it in phases without undue further delay, so that the Customer can meet the 72-hour deadline in Article 33(1).

9.3 Cooperation. The Processor shall cooperate with the Customer and take the reasonable steps the Customer directs to investigate, mitigate and remediate the breach, including by providing the information the Customer needs to notify its supervisory authority and, where required, data subjects. The Processor shall document each breach affecting Customer Data (facts, effects, remedial action) and make the documentation available on request.

9.4 No admission. Notification of, or response to, a breach under this clause is not an acknowledgement of fault or liability by the Processor. The Customer remains responsible for notifying its supervisory authority and data subjects where required.

10. Data subject requests and authority requests

10.1 Self-service. The Customer shall in the first instance use the Services to respond to data subjects' requests: searching contacts and records by name, phone number or email; viewing and exporting a data subject's conversations, records and files (user interface, API, CSV or XLSX export, PDF); rectifying data; restricting processing by adding contact restrictions or switching the AI agent off for a conversation; and erasing contacts, conversations, records and files.

10.2 Requests received by the Processor. If the Processor receives a request from a data subject relating to Customer Data, it shall forward the request to the Customer within five Business Days of receipt and shall not respond substantively to the data subject unless the Customer instructs it to or the

law requires it. Where a request also concerns data of which the Processor is the controller, the Processor handles that part itself. Where the Customer cannot fulfil a request using the Services, the Processor shall provide reasonable additional assistance on written request; it may charge a reasonable fee, communicated in advance, for assistance that is manifestly excessive in scope or frequency.

10.3 Requests from public authorities. If a public authority or court requests Customer Data from the Processor, the Processor shall, unless legally prohibited, (a) inform the Customer without undue delay so that it can seek a protective order or other remedy; (b) direct the authority to the Customer; (c) review the legality of the request and challenge it where there are reasonable grounds; and (d) disclose only the minimum Customer Data required by a request that is binding on it. The Processor keeps a record of such requests and shall inform the Customer without undue delay of any supervisory-authority enquiry relating to Customer Data, unless legally prohibited.

11. Audit and information rights

11.1 Documentation first. The Customer shall in the first instance rely on this DPA and its Annexes, the Privacy Policy, the Sub-processor list at https://bluemarlinchat.com/dpa and any other documentation the Processor publishes, and shall address further questions in writing to info@bluemarlinchat.com. The Processor shall answer reasonable written questions, including security questionnaires, within 30 days of receipt.

11.2 Third-party reports. Where the Processor or a Sub-processor holds a report or certificate issued by an independent auditor or certification body relevant to the processing of Customer Data (for example the ISO/IEC 27001 certificate of the infrastructure provider), the Processor shall make it, or a summary, available on request under confidentiality. The Customer shall consider such reports before requesting an audit.

11.3 Audits. Where the information provided under clauses 11.1 and 11.2 is not sufficient to demonstrate compliance, the Customer, or an independent auditor mandated by it that is not a competitor of the Processor and is bound by confidentiality, may audit the Processor's processing of Customer Data, including by inspection. Unless a supervisory authority requires otherwise or a personal data breach affecting Customer Data has occurred, an audit may take place at most once in any 12-month period, on at least 30 days' written notice specifying scope, proposed dates, auditor and information requested. Audits take place during the Processor's normal business hours, remotely where the scope allows, with minimum disruption to the Processor's operations and subject to the confidentiality obligations of the Agreement. The Customer bears its own costs and its auditor's, and reimburses the Processor's reasonable costs of assistance beyond two person-days per audit at rates communicated in advance.

11.4 Limits. An audit shall not give access to data of other customers, to the Processor's trade secrets or to information whose disclosure would compromise the security of the Services. Access to the premises of the infrastructure provider is governed by that provider's own audit procedures and may be replaced by its ISO/IEC 27001 certification and audit reports. The Customer shall give the Processor a copy of the audit report and treat it as confidential. The Processor shall remedy any material non-conformity identified within a reasonable agreed period. Nothing in this clause limits the powers of a competent supervisory authority.

12. Return and deletion of Customer Data

12.1 Export during the term. Throughout the term, the Customer may export Customer Data at any time without the Processor's involvement through the user interface, the API and the export functions of the Services, including CSV and XLSX export of records and views and PDF generation of pages.

12.2 Export after termination. For 30 days after termination or expiry of the Agreement, or after deletion of the Customer's organization, the Processor shall on written request to info@bluemarlinchat.com make Customer Data available for export in a commonly used, machine-readable format. An organization suspended for non-payment retains read-only access during the retention period and may export its data.

12.3 Deletion. Unless the Customer requests export under clause 12.2, and in any event once that period has elapsed, the Processor shall delete all Customer Data within 30 days after termination or expiry of the Agreement or after deletion of the organization, whichever is earlier. Access by members, API keys, MCP connections, widgets and published share links is removed immediately on deletion of the organization. Copies in backups are deleted as the backups roll off within a further 30 days, so that no copy remains 60 days after the deletion date. The Processor shall not restore Customer Data from a backup after deletion except as necessary to recover from an incident affecting the Services as a whole, in which case the restored data is deleted again promptly.

12.4 Retention required by law. The Processor may retain data it is required to keep by Union or Member State law, in particular Billing Data and invoices that Spanish commercial and tax law require to be kept for six years, and the acceptance evidence in clause 1.4 to the extent necessary to evidence the conclusion of the Agreement. Such data is retained in isolation, is not otherwise processed and is deleted when the retention obligation ends.

12.5 Confirmation. On written request the Processor shall confirm in writing that Customer Data has been deleted in accordance with this clause, stating the date of deletion and the date by which backup copies will have been deleted. The Processor shall procure that Sub-processors delete Customer Data in accordance with the terms agreed with them.

13. General provisions

13.1 Liability. Each party's liability under or in connection with this DPA is subject to the exclusions and limitations of liability in the Terms, which apply in aggregate to all claims under the Agreement and this DPA together. Nothing in this DPA limits either party's liability towards data subjects or supervisory authorities under Articles 82 to 84, or the right to claim back from the other party the part of any compensation paid to data subjects that corresponds to the other party's responsibility (Article 82(5)).

13.2 Term. This DPA takes effect on acceptance under clause 1.3 and remains in force for as long as the Processor processes Customer Data on behalf of the Customer, including the export and deletion periods in clause 12, regardless of termination or expiry of the Terms.

13.3 Governing law and jurisdiction. This DPA is governed by the laws of Spain. Any dispute arising out of or in connection with it is submitted to the exclusive jurisdiction of the courts of the city of Málaga, Spain, without prejudice to mandatory rules of jurisdiction under Applicable Data Protection Law and to data subjects' rights under Article 79.

13.4 Severability. If any provision of this DPA is held invalid or unenforceable, the remaining provisions remain in force and the invalid provision is replaced by a valid provision that comes closest to its purpose.

13.5 Changes. The Processor may update this DPA to reflect changes in law, supervisory-authority guidance, the Services or the Sub-processors engaged, on at least 30 days' notice of a material change by email to the owner of the Customer's organization and by publishing the new version, with its version label and effective date, at https://bluemarlinchat.com/dpa. Changes that reduce the protection of Customer Data or the Customer's rights do not bind the Customer unless it accepts them; the Customer

may instead terminate the Agreement without penalty before the change takes effect. Changes required by law take effect on the date required by law. The version label at the top of this document identifies the version in force.

13.6 Language and notices. This DPA is drafted in English; translations are for convenience only and the English version prevails. Notices to the Processor are sent by email to info@bluemarlinchat.com; notices to the Customer are sent by email to the owner of the Customer's organization as recorded in the Services, and the Customer shall keep those details up to date.

Annex I — Details of processing

Subject matter. The processing of Customer Data by the Processor in providing the Services, a WhatsApp-based customer-communication and CRM platform, to the Customer.

Duration. The term of the Agreement and, thereafter, until deletion of Customer Data under clause 12.

Nature and purpose. Collection, recording, organisation, structuring, storage, retrieval, consultation, use, transmission, dissemination (where the Customer publishes data), alignment, restriction, erasure and destruction of Customer Data as necessary to provide the following features, each a processing activity carried out on the Customer's instructions:

Feature	Processing carried out
Inbox	Sending and receiving WhatsApp messages and media on the Customer's own number(s); storing conversations; in coexistence mode, receiving messages and, where Meta offers it, prior chat history from the WhatsApp Business app
Campaigns	Bulk template messages to recipient lists; delivery and read tracking; opt-out keyword detection; contact restrictions (do-not-contact) and frequency capping
Workspace / CRM	Records in collections with custom fields (text, phone, email, files, location, booking, relations, formulas, pages), views, tags, notes, segments and audiences, sequences; CSV and Excel import
Files	Uploads and message media in private object storage served through time-limited links; logos, avatars and widget configuration on a public CDN host
Pages and publications	PDF documents generated from records; read-only share links to views and pages, optionally password-protected or with expiry; CSV and XLSX export of shared views
Chat widget	Embeddable script on the Customer's website that opens a WhatsApp conversation; fetches its configuration from the CDN, reads the browser language, sets no cookies and stores nothing about the visitor until the visitor writes on WhatsApp
Website analytics (optional add-on)	Cookieless counting of page views on the Customer's website through the embedded script: page, referring site, campaign tags, device type, time on page and an approximate location derived at ingest from the IP address with a database hosted on the Processor's servers; the IP address and browser identification string are never stored and visits are grouped under a daily, non-reversible hash; attribution of a subsequent WhatsApp enquiry to its source (campaign, link or Meta Click-to-WhatsApp ad)
AI agent (customer-facing)	Replies to incoming WhatsApp messages from the Customer's knowledge base (texts, question-and-answer pairs, uploaded documents, pages crawled from URLs the Customer provides) with data access configured per audience; escalation to human staff; can be switched off per organization, audience or conversation
AI assistant for the team (internal)	Chat assistant for staff that reads and writes organization data through audited tools (every call logged with actor, summary of inputs and outcome); destructive actions require confirmation; per-organization memory; saved procedures ("skills") that may run on a schedule; never exposed to end customers
Voice notes	Transcription of incoming WhatsApp voice messages to text

Feature	Processing carried out
Public API and webhooks	Programmatic access through the REST API with scoped API keys; signed outbound webhooks to endpoints designated by the Customer
MCP connections	The Customer's own AI clients connected to its workspace through delegated authorisation with a consent screen (workspace picker, scopes); data read through such a connection flows to the client and the AI vendor chosen by the Customer
Integrations chosen by the Customer	Airtable base import (credentials stored encrypted); Revolut Business transactions synchronised into a collection under the Customer's OAuth consent; Google Maps address autocomplete in the browser; sign-in with Google
Shared sandbox WhatsApp number	A prospect's own phone paired with a BlueMarlin-owned number for evaluation ("join" code; 72-hour pairing renewed on each inbound message; at most 200 outbound messages per organization per day; pre-approved demo templates only); conversations remain in the organization's inbox
Calendar and booking reminders	Scheduled WhatsApp reminders for bookings stored in records

Categories of data subjects. The Customer's staff and other users of its organization; the Customer's customers, leads and contacts, in particular WhatsApp end users; visitors to the Customer's website who start a WhatsApp conversation through the widget or whose visits are counted by website analytics; persons appearing in records stored by the Customer (for example counterparties in bank transactions, persons named in bookings or notes, persons in imported data); participants in an evaluation using the shared sandbox number.

Categories of personal data. Contact data (names, telephone numbers in E.164 format, country, email addresses, postal addresses, custom fields defined by the Customer); WhatsApp messages and media, voice notes and transcripts; campaign recipients and results (delivery, read, opt-out); notes and tags; records of any kind stored by the Customer, which may include bookings, bank transactions synchronised from Revolut Business and data imported from Airtable or CSV/Excel; knowledge-base contents; AI conversation logs and the assistant's memory; files and generated documents; published pages and views; webhook payloads; API request logs.

Special categories. Not intended. The Services are not designed for Article 9 or Article 10 data or children's data; clause 4.4 requires the Customer not to submit such data without a valid legal basis and prior notice.

Frequency. Continuous, for the duration of the Agreement, as determined by the Customer's use of the Services.

Retention. Customer Data is retained for as long as the Customer keeps it in the Services and until deleted by the Customer or under clause 12. The following operational periods apply:

Category	Retention
API request logs	48 hours
Application event log	30 days
Error reports (error monitoring)	7 days
Temporary uploads to the AI assistant	7 days
Sync run ledger (Airtable and Revolut Business)	30 days
Website analytics: individual page views	90 days; daily aggregate counts for the term of the Agreement

Category	Retention
Sandbox pairing	72 hours after the last inbound message
Database backups	Daily; 7 days on the server, 30 days in EU-jurisdiction object storage (rolling)
Data of suspended or terminated organizations	30 days, then deleted; backups roll off within a further 30 days
Billing records (Processor as controller)	6 years, as required by Spanish commercial and tax law

Annex II — Technical and organisational measures

The Processor implements the following measures pursuant to Article 32, verified against the Services as at the effective date. Only the measures listed are represented; the Processor does not claim certifications it does not hold.

1. Physical security and hosting. Application servers and the primary database run on dedicated servers in a data centre in Germany (EU) operated by an ISO/IEC 27001-certified European infrastructure provider, whose certification covers the physical and environmental security and operational processes of the data centre. The Processor's personnel have no physical access to the data centre.

2. Network and transport security. All traffic is encrypted with TLS 1.2 or higher (HTTPS) and HSTS is enforced. Inbound webhooks from Meta and Stripe are signature-verified; outbound webhooks are signed with a per-organization secret. The database server sits on a private network and is not reachable from the public internet. A DDoS-mitigation and content-delivery layer protects the edge; rate limiting and abuse controls apply, including per-organization caps on the sandbox number and throttling of campaign sends.

3. Access control and authentication. Users authenticate with Google OAuth or a one-time code sent by email; no passwords are stored. Session cookies are not readable by scripts and are sent only over encrypted connections. Access within an organization is governed by membership and roles managed by the Customer. Third-party AI clients connect through delegated authorisation with a consent screen and receive scoped, revocable tokens. API keys are scoped and stored only as one-way hashes. Third-party integration credentials are encrypted at rest. Administrative access to production is key-based, limited to named administrators and granted only in time-limited windows; routine diagnostic access to production data is read-only.

4. Tenant isolation and pseudonymisation. Every database query is scoped to the organization of the authenticated user or key (multi-tenant filter). All identifiers are randomly generated and non-guessable, so resources cannot be enumerated. The AI agent's knowledge base, memory and tool access are isolated per organization. Pseudonymous identifiers rather than directly identifying data are used between systems and towards Sub-processors wherever the function permits.

5. Encryption. Data in transit is encrypted as in section 2. File and media storage and backups in object storage are encrypted at rest by the provider. Integration credentials are encrypted at rest; API keys are stored as one-way hashes. Private files are reachable only through time-limited links; only logos, avatars and widget configuration are in public storage.

6. Logging, monitoring and audit. The application event log may contain message content and telephone numbers, so that delivery problems can be diagnosed; it is stored in the same database and region as the Customer Personal Data it describes, and is visible only to the Customer's own organization and the Processor's authorised personnel. Server console output is kept free of telephone numbers and message bodies. Error reports are scrubbed of telephone numbers and message bodies

before being sent to the error-monitoring service, which stores them in the EU region (Germany). Every action taken by the AI assistant through its tools is recorded in an audit log (acting user, tool, summary of inputs, time, outcome); destructive actions require explicit confirmation. Health checks monitor availability. API request logs are kept 48 hours; the event log 30 days.

7. Backup and resilience. The primary database is backed up daily; backups are kept 7 days on the server, protected by the server's access controls, and 30 days in object storage under EU jurisdiction, where they are encrypted at rest by the provider. The restore procedure is documented and rehearsed. During a database incident, inbound WhatsApp webhooks are buffered briefly in the managed cache in Frankfurt so that messages are not lost.

8. Development and change management. Deployments are automatically verified before being built and can be rolled back; health checks verify each deployment. Dependencies are kept up to date. Changes to data structures are reviewed before being applied.

9. Incident management. Personal data breaches affecting Customer Data are assessed, contained and notified to affected customers without undue delay and no later than 48 hours after the Processor becomes aware, with the Article 33(3) information provided as it becomes available (clause 9). Incidents are documented with facts, effects and remedial action.

10. Sub-processor management. Sub-processors are engaged only under written data-protection terms and listed in Annex III with service, data, location and transfer mechanism. Changes are notified at least 30 days in advance (clause 7). Each Sub-processor receives only the data necessary for its function.

11. Data minimisation and AI-specific safeguards. The Services contain no analytics trackers, advertising pixels or third-party tracking. The widget sets no cookies and stores nothing about a visitor until the visitor writes on WhatsApp. AI Sub-processors receive only the text needed for the task (message, relevant knowledge excerpts, conversation context, record content read by a tool) and never Billing Data; their terms exclude use of inputs for training, and the Processor does not use Customer Data to train models. The AI agent can be switched off per organization, audience or conversation, and its data access is configured per audience by the Customer.

12. Personnel and confidentiality. All personnel with access to Customer Data are bound by written confidentiality obligations. Access is limited to named administrators and granted only when necessary, in time-limited windows (section 3).

13. Deletion. Customers can delete contacts, conversations, records, files and organizations through the Services; deleting an organization removes access immediately, erases content within 30 days, and backups roll off within a further 30 days. Operational data is deleted automatically at the end of the retention periods in Annex I. Time-limited file links expire automatically and sandbox pairings 72 hours after the last inbound message.

Annex III — Authorised Sub-processors

The Customer authorises the following Sub-processors under clause 7. The current list, with any notified changes, is published at https://bluemarlinchat.com/dpa.

Sub-processor	Service	Data	Location of processing	Transfer mechanism
European infrastructure provider (ISO/IEC 27001; legal name available on request under confidentiality)	Hosting of application servers, primary database and backups	All platform data	Germany (EU)	Not applicable (processing in the EU)
Cloudflare, Inc.	Object storage (EU jurisdiction setting), CDN, DNS, DDoS protection	Files, media, generated PDFs, public assets; HTTP request metadata at the edge	Storage in the EU; global edge network for HTTP traffic; United States company	EU-U.S. Data Privacy Framework (certified) and SCCs
Upstash, Inc.	Managed cache and resilience buffer	Organization and membership identifiers; transient buffer of inbound WhatsApp webhooks during database incidents	Frankfurt, Germany; United States company	SCCs
Functional Software, Inc. (Sentry)	Error monitoring	Technical error reports, request metadata, IP addresses; telephone numbers and message bodies scrubbed before transmission	EU region (Germany); United States company	EU-U.S. Data Privacy Framework and SCCs
Stripe, Inc. / Stripe Payments Europe, Ltd.	Payments, invoices, subscriptions	Billing contact, card data (never received by the Processor), invoices	Ireland and United States	EU-U.S. Data Privacy Framework and SCCs
Resend, Inc.	Transactional email (one-time sign-in codes, invitations, notifications)	Email address, name, email content	United States	SCCs
Meta Platforms Ireland Ltd / Meta Platforms, Inc. / WhatsApp LLC	WhatsApp Business Platform (Cloud API)	Telephone numbers, message content, media, delivery status, templates	Ireland and United States	EU-U.S. Data Privacy Framework and SCCs; also an independent controller for the WhatsApp service itself
Anthropic, PBC	LLM responses for the AI agent and the internal assistant	Message text, knowledge excerpts, conversation context, record content read by tools	United States	EU-U.S. Data Privacy Framework 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	United States and Ireland	EU-U.S. Data Privacy Framework and SCCs; API terms exclude training on inputs

Sub-processor	Service	Data	Location of processing	Transfer mechanism
Google Ireland Ltd / Google LLC	Sign-in with Google (OAuth); Maps address autocomplete (browser-side, directly against Google)	Email, name and avatar at sign-in; addresses typed into the autocomplete field	Ireland and United States	EU-U.S. Data Privacy Framework and SCCs

Stripe, Resend and Google process mainly Account Data and Billing Data of which the Processor is the controller; they are listed for completeness because invitation emails and sign-in data include names and email addresses of the Customer's users. Data Privacy Framework certification status can be verified at https://www.dataprivacyframework.gov; where a certification lapses, the SCCs concluded with the Sub-processor continue to apply.

Services that the Customer chooses to connect to its organization, namely Airtable, Revolut Business, MCP-capable clients (such as Claude Code, Claude Desktop, Cursor or any other client the Customer configures) and the AI vendors those clients use, together with the endpoints to which the Customer directs webhooks, are independent third parties engaged by the Customer under its own agreements. They are not Sub-processors, and the transfer of Customer Data to them is made by the Customer on its own responsibility.

Annex IV — Data residency statement

The Customer may reproduce the following statement in its records of processing, vendor assessments and communications with its supervisory authority. It reflects clause 6 as at the effective date and is kept current at https://bluemarlinchat.com/dpa.

Bluemarlin Ventures S.L. (tax identification number ESB27665173, Avenida de San Antón 37, 29018 Málaga, Spain) provides the BlueMarlin platform from Spain and processes Customer Data as a processor under Article 28 GDPR.

Customer Data at rest is stored exclusively in the European Union (Germany):

1. Application servers and the primary database, holding all platform data, run on dedicated servers in a data centre in Germany operated by an ISO/IEC 27001-certified European infrastructure provider, whose legal name is available on request under confidentiality.
2. Database backups are taken daily and kept 7 days on the database server and 30 days in object storage under EU jurisdiction, where they are encrypted at rest by the provider.
3. Files, media, voice notes and generated documents are stored in object storage under EU jurisdiction (Cloudflare, EU jurisdiction setting), encrypted at rest by the provider and served through time-limited links.
4. The cache and resilience buffer (Upstash) is hosted in Frankfurt, Germany, and holds organization and membership identifiers and, only during a database incident, a short-lived buffer of inbound WhatsApp webhooks.
5. Error monitoring (Sentry) uses EU data residency in Germany; telephone numbers and message bodies are scrubbed before an error report is sent.

Customer Data leaves the European Union only transiently, in the course of a request, through the sub-processors listed in Annex III and only for: transmission of WhatsApp messages (Meta); generation of AI responses (Anthropic); text embeddings and voice-note transcription (OpenAI); transactional email

(Resend); payment processing (Stripe); sign-in with Google; and the global edge network of the content-delivery and DDoS-protection provider (Cloudflare) through which HTTP requests are routed. These transfers rely on the EU-U.S. Data Privacy Framework where the provider is certified and otherwise on the Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) with a transfer impact assessment and supplementary measures. The AI providers' terms exclude use of inputs to train models, and Bluemarlin Ventures S.L. does not use Customer Data to train models.

Bluemarlin Ventures S.L. will not move the primary storage of Customer Data outside the European Union without at least 30 days' prior notice to the organization owner and publication at https://bluemarlinchat.com/dpa; the Customer may object and terminate without penalty.

Questions about data residency, the identity of the infrastructure provider or this statement: info@bluemarlinchat.com.

Contact

Bluemarlin Ventures S.L.
VAT ESB27665173
Avenida de San Antón 37, 29018 Málaga, Spain
info@bluemarlinchat.com