Data Processing Agreement

Callimacus S.r.l. · Version 2026-11-17 of 17 November 2026

NOVEMBER 11, 2026

DATA PROCESSING AGREEMENT (“DPA”)

APPOINTMENT AS DATA PROCESSOR

This DPA forms an integral and essential part of the Contract and governs the processing of Personal Data carried out by Callimacus S.r.l., having its registered office at Piazzetta dei Sapienti no. 1, Corciano (PG), Solomeo, 06073, Italy, VAT no. 03950820542 (hereinafter “Callimacus” or also the “Processor”), on behalf of the Client, as identified in its account (hereinafter also the “Controller”), pursuant to Article 28 of Regulation (EU) 2016/679 (“GDPR”).

For the purposes of this DPA, the Client acts as Data Controller and Callimacus acts as Data Processor.

In light of the foregoing, the Parties agree as follows with regard to the processing of Personal Data under the Contract, specifying the roles and responsibilities of each Party.

Article 1 – Definitions

The technical and legal terms used in this DPA are set out below; some of these qualifications or definitions are identified, interpreted and, where appropriate, supplemented on the basis of Article 4 GDPR:

“Authorized Persons”: the natural persons authorized to process Personal Data under the direct authority of the Data Controller or of the Data Processor.

“Contract”: the agreement entered into between Callimacus and the Client for the provision of the Callimacus Platform (the “Agreement” or “Contract”), consisting of the Terms and Conditions (“T&C”), the Plans and Pricing Page, the Service Level Agreement (“SLA”), this DPA and any additional Annex, as defined in the T&C.

“Data Controller”: (also the “Controller”) the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

“Data Processor”: (also the “Processor”) the natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

“Data Subject”: the identified or identifiable natural person to whom the Personal Data relate.

“DPA”: this document, referred to in the Contract as the “Data Processing Agreement” or “Data Protection Agreement”, which governs the processing of Personal Data and appoints Callimacus as Data Processor pursuant to Article 28 GDPR.

“Legislation”: (also the “Data Protection Legislation”) means (1) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); (2) the national legislation implementing or supplementing the GDPR or any other legislation in force on the protection of the personal data of natural persons, and in particular Italian Legislative Decree no. 196/2003, as amended; (3) the guidelines, opinions and decisions adopted by the Supervisory Authority, by the Article 29 Working Party on the protection of individuals with regard to the processing of personal data established by Directive 95/46/EC and/or by the European Data Protection Board.

“Personal Data Breach”: (also the “Data Breach”) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

“Sub-processor”: the third party directly engaged by the Data Processor to carry out specific processing activities on behalf of the Data Controller.

Article 2 – Purposes of the Processing, Categories of Data Subjects and Types of Personal Data

2.1 Without prejudice to the rights and obligations of the Processor under this DPA and to Article 2.2 below, by entering into this DPA the Controller entrusts the Processor, which accepts, with carrying out on its behalf the Personal Data processing operations necessary for the proper performance of the Contract, namely for the provision of the Callimacus Platform for building, hosting and serving the Controller’s website, for AI-based browsing assistance and for the personalization and optimization of the user experience on the Controller’s website, for delivering to the Controller the messages that End Users send through the forms of its website, as well as for the security of the Platform, as described in Schedules 1, 2 and 3; these include the following types of operations:

(a) Collection: acquisition of Personal Data;

(b) Recording: recording of Personal Data;

(c) Transmission: sending of Personal Data to a specific recipient;

(d) Erasure: permanent deletion of Personal Data;

(e) Handling: any type of operation performed on Personal Data;

(f) Storage: archiving of Personal Data.

2.2 The processing concerns: (a) as to the categories of Data Subjects, the visitors and End Users of the Controller’s website who use the Callimacus Platform, as well as any natural persons mentioned in the content made available by the Controller; (b) as to the types of Personal Data, the pseudonymous session identifier (UUID) stored in the intent_sid cookie and the interaction data associated with it (intent metadata, urgency and sentiment indicators, contextual browsing data, features of the products viewed, technical device data), the content of text and voice prompts and the images submitted by End Users, the contact details and messages End Users send through the forms of the Controller’s website, as well as the IP address, processed for security purposes and, together with the browser user agent and in the form of a keyed hash whose key is discarded within two days, to group an End User’s interactions into visits; (c) any additional data collected as a result of the Controller’s modification of the default masking configuration (Schedule 3); (d) any Personal Data contained in the Source Website (as defined in the T&C) and in the corporate content and knowledge made available by the Controller for the Platform’s knowledge base. A detailed description is provided in Schedules 2 and 3.

2.3 This DPA applies to any processing of Personal Data connected with the building and changing of the Controller’s website that Callimacus carries out through the Platform (Build, as defined in the T&C).

Article 3 – Duration

3.1 The provisions of this DPA shall remain in force, unless otherwise specified, for the duration of the Contract. However, the Processor shall remain subject to the provisions of this DPA also for the entire period between the termination of the Contract and the actual erasure of the data, as governed by Article 9.

Article 4 – Manner of Processing by the Processor

4.1 The Processor shall process Personal Data solely and exclusively for the purpose of fulfilling its obligations under the Contract entered into with the Controller and shall not process or use Personal Data for purposes other than those indicated by the Controller. Furthermore, the Processor shall limit the use of Personal Data to a period not exceeding that necessary for the purposes for which the data were collected.

4.2 By entering into this DPA, the Processor declares that it has the necessary expert knowledge, reliability, resources, suitability, experience and capabilities required by the GDPR. In particular, pursuant to Article 28

GDPR, the Processor undertakes to comply with, and to ensure that its Authorized Persons comply with, the following instructions regarding the processing of Personal Data:

(a) process Personal Data lawfully and fairly, in compliance with the Legislation and with the written instructions received from the Controller, also ensuring compliance with Article 28 GDPR;

(b) identify and designate the Authorized Persons and provide them with detailed instructions for the correct and lawful processing of Personal Data, supervising their activities;

(c) ensure that the Authorized Persons are bound by appropriate confidentiality obligations and that such obligations continue to apply after the termination of their relationship with the Processor;

(d) not assign, transfer, disclose and/or provide copies, in whole or in part, in any manner and in any format, of Personal Data to third parties, except with specific written authorization and without prejudice to Article 5 below.

4.3 This DPA, its Schedules and the Contract constitute the Controller's documented instructions. This is without prejudice to cases where processing is required by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

The Parties acknowledge that the Callimacus Platform is provided as a standardized service, based on an architecture common to all clients of Callimacus: any instructions on the processing of Personal Data in addition to those set out in this DPA, which the Controller may communicate in writing to Callimacus, shall therefore be carried out within the limits of the configuration options available within the services provided for in the Contract. The Processor's obligations under this DPA and the Legislation remain unaffected. Should the Controller consider further customizations necessary that cannot be carried out within such limits, the Parties reserve the possibility to negotiate them in good faith.

Where the Processor considers that an instruction given by the Controller infringes the applicable Legislation, it shall immediately inform the Controller and may suspend the execution of that instruction until it is confirmed or amended in writing.

4.4 The Controller expressly authorizes the Processor to anonymize the Personal Data processed on its behalf and to use the data so anonymized, as well as aggregated behavioral metrics, for the purposes of security, maintenance, optimization, quality control and improvement of the Callimacus Platform, as described in Schedule 1. Anonymization is carried out in such a way as to prevent the re-identification of Data Subjects. The Controller further authorizes the Processor to use any aggregated, non-identifying data on the use of the Platform that may be necessary to measure the Credits (as defined in the T&C) consumed for the purposes of invoicing and of verifying the service levels provided for in the Contract.

Article 5 – Third Parties Involved in the Processing (Sub-processors and System Administrators)

5.1 The Controller hereby grants Callimacus a general authorization to engage Sub-processors for the proper performance of the contractual services. The Sub-processors listed in Schedule 4 to this DPA are authorized by the Controller with immediate effect.

Callimacus shall inform the Controller, with reasonable prior notice, of any intended changes concerning the addition or replacement of Sub-processors. The Controller may object to such changes on objective, legitimate, specific and documented grounds relating exclusively to data protection, to be communicated within 10 (ten) days of the notice; in the absence of a written objection within that period, the changes shall be deemed accepted. Should the Parties fail to reach an amicable agreement following an objectively irreconcilable objection, either Party shall be entitled to withdraw from the Contract without any penalty or withdrawal fee, without prejudice to payment for the services validly provided up to that time.

5.2 The Processor shall impose on each Sub-processor, by way of contract, data protection obligations identical or equivalent to those set out in this DPA and shall remain fully liable to the Controller for the

performance of its Sub-processors, pursuant to Article 28(4) GDPR.

5.3 Where applicable and necessary in relation to the services provided, the Processor shall formally designate its System Administrators pursuant to the general provision of the Italian Data Protection Authority (Garante per la protezione dei dati personali) of 27 November 2008, as amended.

5.4 Whenever requested by the Controller, the Processor shall provide the Controller with the updated list of the Sub-processors and System Administrators involved in the processing activities.

Article 6 – Security of the Processing

6.1 Pursuant to Article 32 GDPR, the Processor undertakes to adopt technical and organizational security measures designed to ensure the security of Personal Data, in order to prevent any loss of their availability, integrity and confidentiality. The general and technical description of the infrastructure relating to the service covered by the Contract is set out in Schedules 1, 2 and 3 to this DPA: the Controller acknowledges such measures as suitable and appropriate pursuant to Article 32 GDPR.

6.2 At any time, provided that this does not cause serious interference with the Processor's normal business activities, the Controller may request explanations and clarifications regarding the security measures adopted pursuant to this Article 6. The Processor shall provide the Controller with an adequate response without undue delay.

6.3 The security of the data flows exchanged in read/write mode between the Callimacus Platform and the Controller's external IT systems is governed by a principle of shared responsibility. Callimacus guarantees the security measures relating to the IT systems within its own remit; the Controller remains solely responsible for the security of its own IT systems interfacing with the Callimacus Platform, ensuring their compliance with the Legislation.

6.4 The service levels relating to the availability of the Platform, together with the related remedies, and any backup functionality for the Controller's data remain governed exclusively by the Contract. The Processor's obligations under Article 32 GDPR remain unaffected.

Article 7 – Assistance to and Cooperation with the Controller

7.1 By entering into this DPA, the Processor undertakes to cooperate with the Controller in responding to requests for the exercise of Data Subjects' rights under Articles 15 to 22 GDPR. Without prejudice to the fact that the Processor is not required to handle requests for the exercise of Data Subjects' rights on behalf of the Controller and does not have a dedicated channel for this purpose, the Processor undertakes to forward to the Controller, without undue delay, any request received directly from a Data Subject relating to the data processed on behalf of the Controller, refraining from responding to it independently.

7.2 Where the Processor is required to keep a record of processing activities under the Legislation, it shall provide the Controller, upon request, with all the information necessary to assess its accuracy and consistency with the indications provided by the Controller for the activities connected with the proper performance of the Contract.

7.3 Upon request, the Processor undertakes to assist the Controller in preparing and periodically updating the acts and documents required by the Legislation (such as, by way of example only, the data protection impact assessment), taking into account the nature of the processing and the information available to the Processor, by making the information in its possession available to the Controller.

7.4 The Controller has the right to verify the Processor's compliance with its obligations under this DPA, either directly or through an auditor appointed by it, bound by confidentiality obligations and not being a competitor of Callimacus. The Processor shall make available to the Controller the information necessary to demonstrate compliance with such obligations. The Parties agree that this right shall ordinarily be satisfied by making available an audit report, carried out by the Processor or by third parties appointed by it, drawn up less than 12 (twelve) months before receipt of the request. In the event of a Data Breach, of a request from a

Supervisory Authority or of the absence of a suitable audit report within the above timeframe, the Controller may carry out an audit, no more than once per calendar year, except in the event of a Data Breach or of a request from the Supervisory Authority, with at least 30 (thirty) days' prior written notice, during normal business hours and in a manner that does not prejudice the operation and security of the systems or the confidentiality of the data of the Processor's other clients.

7.5 Any assistance provided by Callimacus under Articles 7.3 and 7.4 above which exceeds what is ordinarily provided for in the Contract (such as, by way of example, support in preparing the Controller's DPIA, responding to prior consultations or managing the Controller's audits) shall be borne by the Controller and charged in accordance with the economic conditions set out in the Contract or, failing that, on the basis of a specific quotation approved by the Controller.

7.6 In the event of a Data Breach occurring on Callimacus's systems, the Processor undertakes to notify the Controller without undue delay after becoming aware of it, i.e. from the moment it has a reasonable degree of certainty that a security incident has occurred which has compromised Personal Data processed on behalf of the Controller. Where it is not possible to provide all the information at the same time, the information may be provided in phases without further undue delay. The Processor undertakes to assist the Controller, to the extent possible, for the purposes of:

(a) making, within the time limits and in the manner provided for by law, the notifications to the competent Supervisory Authority pursuant to Article 33 GDPR;

(b) any communication to the Data Subjects, where the circumstances set out in Article 34 GDPR apply.

In order to ensure compliance with the requirements of Article 33 GDPR, the Processor shall provide the Controller with the information in its possession concerning:

(i) the nature of the Data Breach;

(ii) the categories and approximate number of Data Subjects and of Personal Data records concerned;

(iii) the likely consequences and impact of the Data Breach;

(iv) the measures taken or proposed to address the Data Breach or to mitigate its effects;

(v) the name and contact details of the contact point at the Processor;

(vi) any further information and/or documentation reasonably requested by the Controller.

The Processor shall promptly take action to analyze the Data Breach occurring on its systems and to identify appropriate measures to mitigate its effects. The costs of the analysis, recovery and remediation activities shall be borne by the Party to which the Data Breach is attributable, including, for the Controller, cases where the Data Breach arises from systems, configurations or credentials falling within its sphere of responsibility or from the non-performance of its obligations under this DPA; in such cases, the costs incurred by Callimacus shall be charged to the Controller in accordance with Article 7.5. In the event of concurrent causes, the costs shall be allocated in proportion to the respective responsibilities. The allocation of costs shall in no event delay the fulfillment of the information and assistance obligations under this Article.

Article 8 – International Data Transfers

8.1 Where Personal Data are transferred outside the EEA to a third country not covered by an adequacy decision of the European Commission, the Processor shall ensure that the transfer takes place in compliance with Articles 44 et seq. GDPR, by applying an appropriate transfer mechanism (in particular, the Standard Contractual Clauses adopted by the European Commission and any supplementary measures). The current countries of destination and the related safeguards are set out in Schedule 4 to this DPA: the Controller shall be informed of any change in accordance with the procedure set out in Article 5 above.

8.2 The Processor shall also inform the Controller, unless prohibited by law, of any request for access to Personal Data from public authorities of third countries of which it becomes aware.

Article 9 – Erasure of Data

9.1 The Controller hereby chooses, pursuant to Article 28(3)(g) GDPR, that upon termination of the Contract and, in any case, of the processing of data by the Processor, the latter shall erase all Personal Data processed on behalf of the Controller, together with any existing copies, excluding their return. This is without prejudice to any storage required by Union or Member State law and to the technical erasure times of the systems of the Processor and of the Sub-processors (such as security logs and backup copies), during which the data remain protected under this DPA. It is understood that any data that are anonymous within the meaning of the Legislation may be used and retained by the Processor.

Article 10 – Obligations and Rights of the Controller

10.1 The Controller shall comply with the obligations imposed on it by the Legislation and, in particular, shall:

(a) ensure that the information contained in this DPA is accurate and up to date;

(b) ensure that the collection and processing of data comply with the principles of the GDPR and are based on a valid legal basis under Articles 6 and 9 GDPR;

(c) provide Data Subjects with the information notice under Articles 13 and 14 GDPR, covering the processing carried out through the Callimacus Platform and the intent_sid cookie;

(d) integrate into the interface of its website the transparency notice on the interaction with an AI system, using the technical tools and information made available by Callimacus (Article 50(1) of Regulation (EU) 2024/1689 – "AI Act"; Schedule 1, para. 7.1);

(e) diligently apply, or allow the application of, the data-intent-redact="mask" attribute, as described in Schedule 3;

(f) not configure or use the Platform for the processing of special categories of Personal Data (Article 9 GDPR) or of Personal Data relating to criminal convictions and offences (Article 10 GDPR), unless previously agreed in writing with the Processor.

10.2 The Controller undertakes to obtain in advance the consent of the End Users of its website in accordance with the Legislation, through a suitable consent management system (AI/Cookie Banner). The Controller shall indemnify and hold Callimacus harmless from any administrative fine, damage, third-party claim (including claims by Data Subjects) or legal expense arising directly from the failure to collect, or the non-compliant collection of, the consents referred to in this Article 10.2 or from the absence of an appropriate legal basis for the processing of the End Users' data transmitted to the Platform.

Article 11 – Representations and Liability of Callimacus

11.1 By entering into this DPA, the Processor accepts its appointment as Processor pursuant to Article 28 GDPR, confirms its direct and thorough knowledge of the obligations it assumes under the above-mentioned legislation, undertakes to process Personal Data correctly and lawfully for the sole purpose of performing the assignment received and warrants that it has adequate organizational and financial capabilities for the processing of the Controller's Personal Data in compliance with the Legislation. The Processor further declares that it provides sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing meets the requirements of the GDPR and ensures the protection of the rights of the Data Subject.

11.2 To the extent permitted by law and except in cases of willful misconduct or gross negligence, the aggregate liability of Callimacus towards the Controller arising out of or in connection with this DPA, on any grounds whatsoever (including contractual breaches and recourse actions for fines or compensation paid by the Controller), shall in no event exceed the maximum limit set out in the Contract. It remains understood that, pursuant to Article 82(2) GDPR, Callimacus shall be liable for the damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Controller.

Article 12 – Governing Law and Jurisdiction

12.1 The law governing this DPA and the court having jurisdiction over any dispute relating to it shall be those set out in the Contract.

Article 13 – Final Provisions

13.1 This DPA supersedes any other agreement or understanding between the Parties governing the processing of Personal Data for the provision of the services under the Contract. In the event of any conflict between the provisions of this DPA and those of the Contract (or of any Controller documents not expressly accepted by the Processor), this DPA shall prevail.

13.2 Should any provision of this DPA be held invalid, this shall not affect the validity and effectiveness of the remainder of this DPA. The Parties shall endeavor to replace any invalid provisions with valid ones.

13.3 This DPA is closely connected with the Contract, of which it forms an integral part.

13.4 The communications provided for in this DPA, including those under Articles 5.1 and 7.6, shall be sent to the Client at the e-mail address of its account and to Callimacus at support@callimacus.ai or at its certified e-mail address callimacussrl@legalmail.it, in accordance with the Contract.

13.5 In view of the intrinsic features of the Callimacus Platform, the following Schedules to this DPA shall be deemed an integral and essential part of this document:

Schedule 1 – AI Act Report “Callimacus” – Client Version;

Schedule 2 – DPIA Extract – Callimacus – Client Version;

Schedule 3 – Intent_sid Cookie Report – Client Version;

Schedule 4 – List of Sub-processors – Client Version.

The Client accepts this DPA online, together with the T&C, when it subscribes to a Plan.

The Parties declare that this DPA and its Schedules constitute the expression of their contractual intent with regard to the protection of Personal Data. Each Party declares that it has carefully examined each individual clause, has fully understood its legal effects and accepts its entire content without reservation.

Pursuant to and for the purposes of Articles 1341 and 1342 of the Italian Civil Code, the Controller declares that it has carefully read and specifically approves the following Articles of this DPA:

Article 4.3 (Limits on the execution of the Controller’s additional instructions and Processor’s right to suspend the execution of instructions deemed unlawful);

Article 5.1 (General authorization of Sub-processors, deadline for objection and right of withdrawal);

Article 6.1, last sentence (Acknowledgment of the adequacy of the security measures);

Article 6.3 (Controller’s sole responsibility for the security of its own systems);

Article 6.4 (Exclusive reference to the Contract for service levels, related remedies and backup);

Article 7.4 (Limitations on and procedures for audits);

Article 7.6, last part (Allocation of costs in the event of a Data Breach);

Article 10.2 (Indemnity in favor of the Processor);

Article 11.2 (Overall limitation of the Processor’s liability).

Schedule 1 – AI Act Report “Callimacus” – Client Version

“CALLIMACUS”

11.11.2026 (v. 4)

Client version

CONTENTS

1. Introduction and regulatory framework

2. Functional description of the multi-agent architecture

3. Technical specifications and ecosystem integrations

4. Legal qualification of roles and data flows (GDPR/AI Act)

5. Governance of algorithmic learning and data segregation

6. Specific risk assessment and system classification

6.1 Unified classification under Regulation (EU) 2024/1689 (AI Act)

6.2 Mandatory High-Risk exclusion clauses (legal safeguard)

7. Register of compliance obligations and allocation of responsibilities

7.1 Summary table of the main obligations (AI Act) – Scenario: Callimacus as Provider

1. INTRODUCTION AND REGULATORY FRAMEWORK

This document (hereinafter also the "Report") constitutes the impact and compliance analysis of the generative artificial intelligence platform called "Callimacus" (hereinafter the "Platform"), developed by Solomei AI S.r.l., now Callimacus S.r.l. (hereinafter "Callimacus").

Following the evolution of its original cookieless configuration, the Platform now operates natively as a multi-agent architecture that coordinates, in a hybrid configuration, proprietary language models and open-architecture models (see para. 3).

The infrastructure is divided into two logical macro-components:

- back-end component: Callimacus's servers (located in the AWS Region eu-west-1 in Ireland) and the other Sub-processors authorized under the DPA (listed in Schedule 4 to the DPA), which host the core application logic and through which the AI model APIs are queried. Where the Client requests activation of the geolocation service, the Platform integrates with Google Maps Platform, which acts as an independent controller;
- front-end component: the Client's website, generated and hosted by Callimacus through the Platform, which runs directly within the End User's browser (client-side) and communicates with the Callimacus back-end.

For real-time analysis, Callimacus provides an independent software module called a Software Development Kit (SDK). This SDK can also be installed on a standalone basis on the Client's website to track front-end events (clicks, scrolling, browser metadata and text content of HTML pages, etc.). This architecture makes it possible to reconcile and correlate data on the AI-assisted browsing experience. The infrastructure supports only two operating modes, both subject to the End User's consent: (i) in-session AI-assisted browsing and (ii) tracking and personalization through the activation of the proprietary first-party cookie called "intent_sid".

In both cases, AI-based browsing is subject to obtaining the End User's consent to the use of Artificial Intelligence via a pop-up, and this is enforced in a technically binding way.

In the absence of consent, the SDK operates solely within the limits permitted by the legislation, excluding Personal Data and any data that may allow the End User to be identified, even indirectly.

When the End User gives specific consent, the intent_sid cookie is activated; it works by storing a pseudonymous session identifier (generated as a random alphanumeric Universally Unique Identifier – UUID – string, not derived from the IP address or from hardware or device fingerprinting characteristics) with a

standard default duration (default of 30 days), freely configurable by the Client according to its business policies; the intent_sid cookie is provided with the necessary security attributes such as SameSite=Lax and Secure for encrypted HTTPS connections.

If the End User withdraws consent to the use of AI, the SDK immediately stops running, removes the intent_sid cookie from the End User's browser (where activated) and permanently discards, directly on the client, all material and data collected up to that point in the session, preventing them from reaching the back-end.

This analysis has been prepared to map and manage the risks arising from Callimacus's market positioning:

- role of "Provider" pursuant to Article 3, point (3) AI Act, in relation to the provision of the Platform on a Software-as-a-Service (SaaS) basis to Clients for integration into their respective digital ecosystems, as well as of Data Processor pursuant to Article 4, point (8) GDPR.

The mapping of roles under the GDPR, together with the qualification of roles under the AI Act, is the prerequisite for the allocation of the responsibilities described in this Report.

2. FUNCTIONAL DESCRIPTION OF THE MULTI-AGENT ARCHITECTURE

The Platform is a multi-agent system in which each component performs a specific function within a coordinated ecosystem.

Below is a brief description of the Agents operating on the Platform, setting out – for each of them – its role, technical function and specific features within the system.

1. SOCRATE | "I know that I know nothing"

the knowledge base, learns from texts, images, audio, video, and rich content

Role	Interprets and understands End User requests by adopting a dialogic approach.
Technical function	Linguistic and semantic analysis of prompts; interpretation of the textual context and of the End User's conversational intent in order to provide the other agents with the most relevant information; natural dialogue management.
Specific features	Introduces a human-centric element into the way the AI "listens", favoring genuine understanding over automatic responses.

2. DEMOSTENE | "Identity"

it interprets and maintains the right tone of voice, faithful to each brand

Role	Responsible for the brand voice: identity, tone, communication style.
Technical function	Standardizes language; ensures multilingual and multicultural consistency; adjusts the communication register according to the context of use and the interface.
Specific features	Ensures that all generated content is recognizable as part of the project's identity, strengthening the website's consistency and user trust.

3. THEANO | "The Architect"

the architect, oversees and controls the entire infrastructure, ensuring its performance

Role	Coordinates the system architecture: organizes and orchestrates the dialogue between the internal agents.
Technical function	Request routing; coordination of language models; optimization of computational resources; monitoring and streamlining of the operational flow.
Specific features	Acts as an enabling, cross-cutting layer of the architecture: maintains the efficiency, scalability and overall consistency of the system; makes the model interoperable with the various modules in real time.

4. THAMYR | “The Paintress”

our “paintress”, she crafts each experience in real time, reading user intent and adapting content and UX accordingly

Role	Turns the End User’s intent into a fully personalized, instant and unique experience.
Technical function	Guides the End User’s dynamic navigation on the website; composes interfaces and content in real time; shapes the information space in response to the End User’s intent and in particular which elements to show, with what priority and according to what presentation logic.
Specific features	It is the key to moving beyond the static paradigm of web pages: content “moves” and adapts to the End User as they consume content and interact, helping to make the experience more relevant, fluid and personalized.

5. SKESIS | “Correlation”

the correlation agent, it guides each visitor in the discovery of content and products

Role	Guides End Users in discovering content and products; suggests additional content to enrich the user experience.
Technical function	Maintains narrative consistency between responses; controls the narrative progression of content; avoids repetitions or contradictions; optimizes the duration and quality of the experience.
Specific features	Encourages smooth navigation without narrative breaks; supports and develops a consistent and progressive experience, enhancing user engagement.

6. THE DIOSCURI | “Protection”

the guardrails, they protect interactions from toxic content and advise on enriching the knowledge base

Role	They are the Agents responsible for protecting the integrity of the dialogue between the End User and the Platform.
Technical function	They monitor requests and the course of the interaction in real time, intercepting inappropriate language and inputs and content inconsistent with the conversational parameters or brand values; where necessary, they redirect, limit or stop the dialogue, acting as a “conversational guardrail”.
Specific features	They ensure a respectful and safe environment consistent with the brand identity.

7. PHANTOM | “Privacy by design”

the redaction agent, helps protect visitor privacy

Role	Where enabled for the project, redacts names and surnames (and e-mail addresses containing them) accidentally entered by the End User in the prompt bar.
Technical function	Phantom is optional and can be enabled for each project. Its filtering operates exclusively on the text content of prompts, detecting and redacting names and surnames (and e-mail addresses containing them) in real time; it does not detect all categories of Personal Data. The data that Phantom acts on are exclusively those entered in the prompt, and they are processed without session identifiers, user accounts, behavioral metadata or browsing history.
Specific features	Contributes to compliance with the principles of privacy by design and data minimization.

8. ANTEATER | “Integration and Ingestion Layer”

the integration & ingestion layer, syncs content and powers internal knowledge bases

Role	The Agent in charge of back-office operations, responsible for synchronizing information flows; it feeds the internal knowledge base.

Technical function	Manages the logical connectors, APIs and back-office SDKs; runs content synchronization procedures, indexes document bases and securely feeds the vector databases.
Specific features	It is the secure bridge between the Client's databases and the protected knowledge base used in real time by the front-office conversational agents.

Inferences on urgency and sentiment

The agents draw transient algorithmic inferences from the End User's writing style (e.g. level of urgency of the request), for the sole purpose of calibrating the tone of the assistant's response.

Self-learning

With regard to self-learning, the Callimacus agents continuously analyze interactions in real time, identifying recurring patterns, emerging preferences and friction points in the user journey. The LLMs and generative AI models integrated into the Platform allow the system to constantly update its understanding of End User behavior, adapting content in an increasingly relevant and personalized way.

This process results in an autonomous evolution of the digital experience: the Platform can dynamically rearrange the layout of content, change the interaction style or generate new information solutions based on the inputs collected. The result is a dynamic environment that can progressively transform itself according to the End User's actual needs, ensuring a smooth, responsive and constantly improving experience.

In order to ensure full compliance with Chapter II and Chapter III of the AI Act, it is specified that this self-learning activity does not involve any alteration or autonomous updating of the core weights of the LLMs. The system operates exclusively through dynamic optimization of the application context, and self-learning remains confined to the system itself. Any release of logical or behavioral variants of the agents is subject to a human validation and oversight procedure (Human-in-the-loop) aimed at preventing algorithmic drift or the emergence of discriminatory bias.

3. TECHNICAL SPECIFICATIONS AND ECOSYSTEM INTEGRATIONS

The Platform consists of an integrated multi-agent architecture (8 specialized software agents). The system has no static operating modes: interaction with the End User involves real-time semantic and behavioral analysis of communicative intent and dynamic client-side recomposition of commercial interfaces and layouts. As regards language models, the architecture operates in a hybrid configuration: the language and embedding models are reached through the OpenRouter routing service, which sends each request to the provider hosting the model: Google's Gemini models for the default chat responses and for embeddings, OpenAI's models (hosted by OpenAI or Microsoft Azure) for other language functions and embeddings, TypeSafe's models for screening and composing responses, and Groq's and Cerebras's computing infrastructure for very low-latency execution and inference of open-architecture models; sparse embeddings are computed on an inference endpoint operated by Hugging Face in the AWS Region eu-west-1, and OpenAI's moderation model is called directly. Anthropic's models are used only to build and change the Controller's website. The reranking of search results by relevance is performed with the Cohere Rerank 3.5 model through Amazon Bedrock in the AWS Region eu-central-1 (Frankfurt): AWS acts as processor and Cohere receives no Personal Data. The vector indexes (Pinecone) are hosted in the AWS Region eu-west-1 (Ireland).

For the purposes of personalizing the browsing experience and optimizing conversion rates, the system integrates, subject to the End User's specific consent, pseudonymized tracking through the proprietary "intent_sid" cookie and interfaces with the data made available by the Client.

Groq's infrastructure supports certain back-end processing operations governed by the Platform's multi-agent logic (interpretation of requests, rephrasing of knowledge base queries, generation of responses, processing of front-end display parameters).

Groq also provides the transcription service (Speech-to-Text) for voice input, which the End User can activate only through a positive action (click-to-record) preceded by an informative micro-notice; the transcribed text is

then processed as described above.

4. LEGAL QUALIFICATION OF ROLES AND DATA FLOWS (GDPR/AI ACT)

Scenario: provision of the Platform to Clients (SaaS model)

Framework	Callimacus	Client (e.g. the e-commerce website owner)
AI Act	Provider	Deployer
GDPR	Data Processor (Article 28 GDPR)	Data Controller

5. GOVERNANCE OF ALGORITHMIC LEARNING AND DATA SEGREGATION

The Platform's Machine Learning model continuously analyzes general usage patterns for the purpose of optimizing the system.

In order to ensure complete separation of data between the different Clients (multi-tenant isolation):

1. volatile session data and data stored in the Clients' individual CDPs remain logically segregated in their respective cloud spaces (AWS infrastructure located in the EEA, through segregated and encrypted multi-tenant logical environments) and are never shared between different companies;

2. the Platform's centralized self-learning applies exclusively to aggregated behavioral metrics and abstract, previously anonymized strings, reducing the likelihood of cross-contamination or industrial/commercial leaks between competing tenants to a negligible residual level of risk.

6. SPECIFIC RISK ASSESSMENT AND SYSTEM CLASSIFICATION

6.1 Unified classification under Regulation (EU) 2024/1689 (AI Act)

The Platform is unambiguously classified as a Limited-Risk Artificial Intelligence System (Article 50 AI Act).

This classification is determined by the presence of:

- Generative / Conversational AI systems: the Platform interacts directly with End Users who are natural persons and generates text content, triggering the transparency obligation (Article 50(1) AI Act).
- Recommendation and dynamic personalization systems: the Platform adapts the user interface based on the End User's semantic intent. This functionality does not fall within the High-Risk categories (Annex III AI Act) and does not entail any obligations beyond the transparency obligations under Article 50 AI Act.

6.2 Mandatory High-Risk exclusion clauses (legal safeguard)

In order to ensure that the use of the Platform by Clients (Deployers) does not inadvertently slip into the High-Risk categories (Chapter III and Annex III AI Act) or into prohibited AI practices (Chapter II, Article 5 AI Act), the Contract (in particular the T&C) imposes the following absolute prohibitions on use.

It is strictly prohibited to configure or feed the Platform for:

1. Creditworthiness and reliability/solvency assessment (Credit Scoring): The Platform must not be connected to decision-making systems aimed at establishing the solvency of a natural person or determining their credit score.

2. Discriminatory Dynamic Pricing based on "vulnerability": the personalization of commercial layouts must under no circumstances result in an algorithmic price variation based on profiling of the End User's socio-economic, psychological or health vulnerabilities, age group, disability or psycho-physical conditions. It is understood that the Platform has no technical features for dynamically changing or differentiating the price lists of the products and services displayed.

3. Personnel selection, HR and worker management: The Platform may not be integrated into e-recruitment platforms or used to analyze performance, filter applications or take promotion/disciplinary decisions concerning the staff of Clients.

4. Insurance risk assessment: use for calculating premiums or assessing risks in life and health insurance policies is prohibited.

5. Emotion recognition in the workplace or in education: use of the agents' algorithmic inferences in school, academic or workplace settings is prohibited.

7. REGISTER OF COMPLIANCE OBLIGATIONS AND ALLOCATION OF RESPONSIBILITIES

In order to ensure full accountability of the Platform, the main obligations laid down by the AI Act (Regulation (EU) 2024/1689) are mapped below.

Key: • O = Legal obligation.

7.1 Summary table of the main obligations (AI Act) – Scenario: Callimacus as Provider

Regulatory area	Description of the obligation	Type	Main party responsible	Required action and legal safeguard
AI Act – Article 50(1)	AI disclosure transparency obligation: inform the End User that they are interacting with an AI system.	• O	Callimacus (Provider), with the cooperation of the Client (Deployer)	Callimacus designs the system so that the End User is informed of the interaction with an AI system and provides the Client with the necessary technical information (transparency widget). The Client, under its own responsibility, integrates the notice into the interface of its website, using the widget and the technical information made available by Callimacus and ensuring that the information is provided in a clear manner and at the latest at the time of the first interaction.
AI Act – Article 50(2)	Transparency on content generation: mark the system's output (recommendations/texts) in a machine-readable format.	• O	Callimacus (Provider)	Insertion of invisible metadata into the output of the multi-agent architecture.

Schedule 2 – DPIA Extract – Callimacus – Client Version

CALLIMACUS S.R.L.

Processing: AI-assisted browsing and personalization via the intent_sid cookie

11.11.2026

Client version

0. OVERVIEW OF THE PROCESSING

Preliminary note. This extract is a basis that Callimacus S.r.l. makes available to Clients for drafting the DPIA (assistance under Article 28(3)(f) GDPR and Article 7.3 of the DPA).

EDPB template field	Extracted content
0.1 Controller	The Client, the company or consumer that owns the website integrating the Platform
0.2 Processor	Callimacus S.r.l. (formerly Solomei AI S.r.l.)
0.2 Sub-processors	The Sub-processors listed in Schedule 4 to the DPA, including AWS (region eu-west-1, Ireland) for hosting and (region eu-central-1, Frankfurt) for reranking via Amazon Bedrock.

EDPB template field	Extracted content
0.2 Google Maps Platform	Only if the Client enables physical geolocation; identified as an independent controller.
0.3 Name of the processing	AI-assisted browsing and personalization via the first-party cookie "intent_sid".
0.5 Reasons for the DPIA	WP248 criteria potentially met: evaluation/profiling (intent scoring), large-scale data, innovative technologies (multi-agent generative AI), possible combination of datasets (Client's CDP).
0.5 Scope of the DPIA	SDK, intent_sid cookie, AI agents, text and voice prompts, sub-processors, security IP logs.

1. SYSTEMATIC DESCRIPTION OF THE PROCESSING

The processing consists of multi-agent AI-assisted browsing and content personalization based on a pseudonymous identifier (UUID); a first-party cookie makes it possible to track the End User's behavioral information, with a default duration of 30 days.

1.1.a Personal Data processed

Data	Details	Data Subjects	Special categories
Intent scoring	Probability score of the End User's interest (purchase propensity, support request, search for specifications).	End Users.	No.
Urgency and sentiment indicators	"Transient" inferences drawn from writing style, to calibrate the assistant's tone.	End Users.	No.
Contextual browsing	Pages visited, time spent on product pages, click sequence.	End Users.	No.
Products viewed	Product ID, category, price range, variants.	End Users.	No.
Technical device data	Browser, operating system, device category.	End Users.	No.
Text prompts	Typed text; where Phantom is enabled for the project, names and surnames (and e-mail addresses containing them) are redacted from the text.	End Users.	Possible if entered by the End User.
Voice prompts (audio files)	Click-to-record activation with micro-notice; audio sent to Groq for transcription.	End Users.	Possible if entered by the End User.
Full IP address	Only for security and cyber defense, segregated from browsing data.	End Users.	No.
Identifying form fields (name, e-mail, phone, address, payment card, date of birth, gender, webauthn: 36 fields)	Excluded by default through masking; collected only if the Client changes the configuration.	End Users.	Possible only after a change by the Client.

1.1.b Purposes

#	Purpose	Data involved
1	In-session AI-assisted browsing (without storing the identifier)	Prompts, page content.

#	Purpose	Data involved
2	Semantic personalization of the user experience	UUID, intent scoring, sentiment, browsing, products, technical data.
3	Conversion rate optimization	Pseudonymized tracking via intent_sid and data made available by the Client.
4	Security, threat detection, perimeter defense	Full IP.
5	Physical geolocation (optional)	GPS coordinates.

1.1.c Secondary uses

Use	Stated conditions
Centralized self-learning of the Platform	Only on "aggregated behavioral metrics and abstract, previously anonymized strings"; no updating of LLM weights; releases subject to human validation.

1.1.d Nature, scope and context

Item	Extracted content
Nature	Client-side SDK that, in the absence of consent, operates solely within the limits permitted by the legislation, excluding Personal Data and any data that may allow the End User to be identified, even indirectly; subject to consent, it tracks clicks, scrolling and metadata; 8 AI agents (Socrate, Demostene, Theano, Thamyr, Skesis, Dioscuri, Phantom, Anteater); dynamic recomposition of the interface.
Scope: volumes, number of Data Subjects, geographical area	Website browsing, high volume of End Users, geographical area not determinable.
Context: sector of use	Browsing assistance.
Transfers outside the EEA	Non-EU inference Sub-processors for prompt text; server-to-server calls from the EU cloud (End Users' IP addresses are not transmitted).

1.2 Functional description (flow)

1. Access to the website. In the absence of consent, the SDK operates solely within the limits permitted by the legislation, excluding Personal Data and any data that may allow the End User to be identified, even indirectly.

2. Consent to AI (pop-up). Enables in-session assisted browsing, without storing the identifier.

3. Specific consent to personalization. Links the UUID to the intent_sid cookie (30 days) and to interaction data.

4. Prompt. Where Phantom is enabled for the project, names and surnames (and e-mail addresses containing them) are redacted from the text; the audio goes to Groq for transcription.

5. Processing by the language models. The text is processed by the inference sub-processors: Groq (open models), OpenAI (chat and embeddings) and Anthropic (LLM functionality); search results are reordered by relevance via Amazon Bedrock (AWS eu-central-1, Frankfurt).

6. Output. Content and layout on the client side.

7. Withdrawal. Removal of the cookie and discarding of the data on the client, without passing through the back-end.

1.3 Means and architecture

Component	Content
Back-end	Callimacus servers on AWS eu-west-1 (Ireland), segregated and encrypted multi-tenant environments.
Front-end	Developed or integrated by the Client, running in the browser.
Models	Hybrid configuration: OpenAI (chat and embeddings), Groq (open models), Anthropic (LLM functionality); Cohere Rerank 3.5 for reranking, used via Amazon Bedrock (AWS eu-central-1, Frankfurt): AWS acts as processor and Cohere Inc./Cohere Technologies Inc. receives no Personal Data.
Database	Pinecone (vector, indexes hosted on AWS eu-west-1, Ireland); ClickHouse.

2. ANALYSIS OF THE PROCESSING

The legal basis is consent, at two levels (AI and personalization), technically enforced, and legitimate interest for security (IP).

2.1.a Legal basis

Purpose	Stated basis
AI-assisted browsing	Consent via pop-up, "enforced in a technically binding way".
Personalization (intent_sid)	Specific consent.
SDK operation without consent	Solely within the limits permitted by the legislation; Personal Data are excluded.
Security (IP)	Legitimate interest.
Physical geolocation	Browser system permission if “requested”.

2.2.a Minimization and retention

Data	Stated measure / retention
intent_sid cookie	30 days by default, configurable by the Client.
Text and voice prompts, transcripts	Processed by Groq, OpenAI and Anthropic, and via Amazon Bedrock for reranking; use by Groq (including transcription of voice prompts) under Zero Data Retention.
Security IP logs	Datadog: 90 days for suspicious requests; underlying traces 15 days.
Form fields	Masking by default (36 fields).
Recipients	Sub-processors (Schedule 4 to the DPA).

2.2.b Sub-processors and transfer safeguards

The table summarizes, for each supplier, the mechanism legitimizing the transfer outside the EEA (Articles 44-50 GDPR) and the contractual safeguards on access to data by third-country public authorities, as stated in the suppliers’ DPAs and contractual terms.

Supplier	Transfer mechanism	Safeguards on requests from public authorities	Technical measures and open points
Amazon Web Services Amazon Web Services EMEA SARL (Luxembourg) / Amazon Web Services, Inc. (USA)	SCCs incorporated into the AWS DPA via the AWS Service Terms; Amazon Web Services, Inc. is also certified under the EU-U.S. Data Privacy Framework (DPF).	SCCs: Cl. 14(b), (c), (e); Cl. 15.1(b); Cl. 15.1(c)-(d); Cl. 15.2. Supplementary Addendum to the AWS DPA: §1.1 redirection of the request to Callimacus; §1.2(a) notification to Callimacus and commitment to seek a waiver where notification is prohibited; §1.2(b) challenge of requests that are excessive or conflict with EU law; §1.3 disclosure of the minimum necessary; §3 warranty that the applicable	Hosting in region eu-west-1 (Ireland); reranking via Amazon Bedrock in region eu-central-1 (Frankfurt).

Supplier	Transfer mechanism	Safeguards on requests from public authorities	Technical measures and open points
		legislation does not prevent compliance with its obligations.	
Anthropic Anthropic Ireland, Limited (EEA contracting entity) / Anthropic, PBC (USA)	Anthropic DPA (24.2.2025) §I.1: SCCs Modules 2 and 3 (Cl. 14, 15.1, 15.2).	No specific clause on requests from public authorities. §I.4: on request, provides the information needed for the Transfer Impact Assessment (the only contractual support for the TIA, and only on request).	Anthropic DPA, Schedule 2: AES-256 encryption at rest and TLS 1.2+ in transit.
ClickHouse ClickHouse Cloud (ClickHouse, Inc., San Francisco, USA)	ClickHouse DPA (10.4.2026) §6.5: as long as the DPF certification is valid, the transfer is not “Restricted” and the SCCs do not apply.	§8.3: redirection to Callimacus, notification within the limits of the law, cooperation to oppose or limit the request (at Callimacus’s expense).	§6.1: processing outside the EU Region selected by Callimacus only where reasonably necessary to provide the services or to comply with legal obligations or binding orders.
Datadog Datadog, Inc. (USA)	Datadog DPA §10.1: SCCs Modules 2 and 3, Irish law; importer Datadog, Inc. (USA). Datadog, Inc. is also certified under the DPF.	No specific clause on requests from public authorities: coverage relies on the SCCs, Cl. 14, 15.1(b), 15.1(c)-(d), 15.2.	Datadog DPA, Appendix B: encryption at rest and in transit, need-to-know access, logical segregation of data.
Google Maps Platform Google Ireland Limited / Google LLC (USA)	Controller-Controller Data Protection Terms (v.11, 7.5.2026): Appendix 1, Part A: §5.3 transfer to Google Ireland not subject to SCCs (EEA country); §4.3(d) transfer to certified Google entities in the US based on the DPF.	No clause on requests from public authorities.	Google acts as an independent data controller (only if the Client enables physical geolocation).
Groq Groq UK Limited (EMEA contracting entity) / Groq LLC (USA)	Groq DPA (15.10.2025) §8.2: SCCs Modules 2 and 3 (Cl. 14, 15.1, 15.2).	§3.2: prompt notification of government requests, unless prohibited by law; challenge of access requests and of related confidentiality obligations. §2.3(c): advance notice of legal obligations, unless prohibited.	Groq DPA, Annex II: encryption at rest and in transit, access audit trail.
OpenAI OpenAI Ireland Ltd (EEA contracting entity) / OpenAI OpCo, LLC (USA)	OpenAI DPA (1.1.2026) Schedule 1 §8.1: SCCs Modules 2 and 3 (Cl. 14, 15.1, 15.2).	§2.2: notification of binding requests from public authorities “to the extent permitted by law”. §2.1: advance notice of legal obligations, unless prohibited. No specific commitment to challenge requests beyond Cl. 15.2.	§2.5 refers to generic security measures.
Pinecone Pinecone Systems Inc. (USA)	Pinecone DPA §11.3: SCCs Modules 2 and 3. §11.2: the DPF may replace the SCCs; in that case Cl. 14 and 15 do not apply.	§6.3: redirection of the request to Callimacus and advance notice so that Callimacus can seek protective measures, unless prohibited by law. §11.6.3: notifications under Cl. 15.1(a) go to Callimacus, not to Data Subjects.	Indexes hosted on AWS eu-west-1 (Ireland).

SCC references (Decision (EU) 2021/914). Cl. 14: assessment of the third country’s laws and practices ((b) circumstances of the transfer, (c) information support to the exporter, (e) notification of changes in the legislation). Cl. 15.1: obligations on requests from public authorities ((a) notification, (b) best efforts to obtain a

waiver of a prohibition on notification, (c) periodic information on requests received, (d) retention of that information). Cl. 15.2: review of the legality of the request, challenge and disclosure of the minimum necessary.

2.3 Measures supporting compliance

Area	Stated measure
Transparency	Cookie notice with name, duration, purpose, data, domains, opt-out; micro-notice for voice; AI notice under Article 50(1) AI Act: designed by Callimacus (Provider) and shown by default in the interface of the Client's website.
Granular consent	Separate consent for the use of AI and for personalization (intent_sid cookie).
Withdrawal	Opting out removes the intent_sid cookie and stops the collection.
Data Subject rights	The Client must have a DSR channel.
Article 28 relationship	Callimacus acts as Data Processor under the DPA.
Transfers	Server-side shielding (the full IP address is collected exclusively for security and cyber defense purposes and is processed in segregation from the other browsing data relating to the End User, making reconciliation impossible) and logical shield (for processing prompt text, the Callimacus back-end makes the server-to-server calls to the non-EU inference Sub-processors, whose servers record only the static IP address of Callimacus's European cloud and not the real IP address of the End User).
Privacy by design / by default	Masking by default, Phantom, non-fingerprinting UUID, discarding of data on the client upon withdrawal, IP segregation.
Security (Article 32)	AWS EEA, segregated and encrypted multi-tenant environments; HTTPS; separate API credentials for the processing of display parameters on the front-end (least privilege); Dioscuri guardrail.
Restrictions on use	Prohibitions under the Contract (T&C): credit scoring, discriminatory dynamic pricing, HR/recruiting, life/health insurance risk, emotion recognition in the workplace/at school.

Threats emerging from the documents (to be validated and rated by the Client, as Data Controller, in its DPIA)

Likelihood, severity and risk level are to be assigned by the DPIA team according to the chosen methodology.

#	Threat	Element of the document from which it emerges	Potential impact on Data Subjects
R1	Behavioral and inferential profiling beyond expectations.	Intent scoring, urgency and sentiment indicators, history, price range linked to the UUID for 30+ days.	Loss of control.
R2	Collection of identifying data due to a configuration change by the Client.	Masking of the 36 fields (including payment cards) can be disabled.	Mass collection of PII and payment data.
R3	Unsanitized audio sent to Groq.	Phantom operates only on text; the audio is transmitted in full for transcription.	Voice and identifying content held by a non-EU third party.
R4	Transfers outside the EEA.	Suppliers involving possible transfers outside the EEA: Amazon Web Services (US provider certified under the DPF, data in the EU Regions eu-west-1 and eu-central-1), Anthropic, ClickHouse, Datadog, Google Maps (if selected), Groq, OpenAI, Pinecone (US provider, indexes in the EU).	Access by third-country authorities, lower level of protection.

#	Threat	Element of the document from which it emerges	Potential impact on Data Subjects
R5	Personal Data in text prompts not redacted.	Phantom is optional per project and only redacts names, surnames and e-mail addresses containing them; other Personal Data entered by the End User reach the inference sub-processors.	Disclosure of personal (possibly special-category) data to third parties, including non-EU.
R6	Unauthorized access or data breach on the back-end, Pinecone or ClickHouse.	Client data and session data in the Platform's cloud systems.	Loss of confidentiality.

4.2 MEASURES ALREADY IN PLACE AGAINST THE RISKS

The following measures are implemented by Callimacus. Some of them depend on the project configuration or on the Client's integration (in particular Phantom, which is optional per project, the default masking of form fields and the collection of consents).

Measures
Double consent; prohibitions on high-risk uses; human-in-the-loop on releases.
Masking by default (data-intent-redact).
Phantom where enabled for the project (names, surnames and e-mail addresses containing them), prompts without session identifiers.
Click-to-record with micro-notice.
Server-to-server logical shield (End User IP not transmitted).
Aggregated and anonymized data only; no changes to LLM weights; multi-tenant segregation.
Exclusion of Personal Data when the SDK operates without consent.
Deletion by the End User; withdrawal.
AWS EEA, encryption, segregation, HTTPS, separate credentials, IP segregation.

Schedule 3 – Intent_sid Cookie Report – Client Version

CALLIMACUS S.R.L.

Operation, features and compliance – 11.11.2026 (v. 3)

Client version

INTRODUCTION

This document sets out, in summary form, the information on the operation, features and compliance of the intent_sid cookie used by the Callimacus platform (the "Platform"), provided on a SaaS basis by Callimacus S.r.l. ("Callimacus")

1. EXECUTIVE SUMMARY

Item	Value
Cookie name	intent_sid (custom, first-party)
Duration	30 (thirty) days by default, which the Client may configure differently (unless deleted earlier by the End User)
Domains of use	Websites of Clients using the Platform on a SaaS basis
Main purpose	Personalization of the user experience

Item	Value
Legal basis	Consent

2. ACTIVATION AND OPERATION

Activation of the intent_sid cookie is subject to the End User giving specific consent and involves tracking activities in order to personalize the browsing experience. Without the specific consent, the intent_sid cookie is not activated: with consent to the use of Artificial Intelligence only, assisted browsing takes place in-session without storing the identifier; in the absence of any consent, the SDK operates solely within the limits permitted by the legislation, excluding Personal Data and any data that may allow the End User to be identified, even indirectly. If the specific consent is withdrawn, the intent_sid cookie is removed and the data collected up to that point are permanently discarded on the client.

When a session is first activated, a unique session identifier (UUID) is generated and stored in the intent_sid cookie with a standard default duration of 30 days (unless configured otherwise by the Client).

3. CATEGORIES OF PERSONAL DATA PROCESSED AND SANITIZATION AND ANONYMIZATION LOGIC

3.1 Automatically excluded data

In line with the principles of data minimization and privacy by design, through the masking process (data-intent-redact="mask"), the fields listed below are masked and therefore not collected at source by default. The Client may change this configuration: only in that case can the SDK capture the fields listed below in forms and HTML elements (including autocomplete hints such as name, address-level1, etc.):

Field	Description	Field	Description
name	full name	country	country code (e.g. IT)
given-name	first name	country-name	country name
additional-name	middle name	postal-code	postcode
family-name	surname	cc-name	cardholder
nickname	nickname/alias	cc-given-name	cardholder's first name
username	username	cc-family-name	cardholder's surname
email	e-mail address	cc-number	card number
tel	telephone number	cc-exp	expiry date (full)
organization	company/organization	cc-exp-month	expiry month
organization-title	role/position	cc-exp-year	expiry year
street-address	full address	cc-csc	CVV/CVC
address-line1	address line 1	cc-type	card network
address-line2	address line 2	bday	date of birth
address-line3	address line 3	bday-day	day
address-level1	region/state/province	bday-month	month
address-level2	city/municipality	bday-year	year
address-level3	district/area	sex	gender
address-level4	sub-area	webauthn	authentication credentials/indicators

Additional HTML elements can also be excluded using the custom attribute data-intent-redact, for example:

```
<div>
   This will be captured
   <div data-intent-redact="mask">This will NOT be captured</div>
</div>
```

3.2 Data collected for semantic personalization purposes

The intent_sid cookie stores a unique session identifier to which the following data on the End User's interaction with the website are linked:

- intent metadata (Intent Scoring): the statistical probability score associated with the End User's interest (e.g. purchase propensity, technical support request, search for technical specifications);
- urgency and sentiment indicators: transient algorithmic inferences drawn from the End User's writing style (e.g. level of urgency of the request), for the sole purpose of calibrating the tone of the assistant's response;
- contextual browsing data: history of the pages visited within the website, time spent on product pages and sequence of clicks made during the active session;
- features of the products viewed: product ID, product category, price range and variants in which the End User has shown interest;
- technical device data: browser type, operating system and device category (mobile/desktop) to optimize the chat's graphic layout.

Minimization and integrity note: the data listed above contain no direct identifiers (first names, surnames, e-mails, credentials, banking data): form fields and HTML elements are in fact excluded according to the masking configuration (para. 3.1).

3.3 Expressly provided exclusions

- IP addresses (excluded from the data linked to the intent_sid cookie – Server-Side Shielding): the full IP address is collected for security and cyber defense purposes and is processed in segregation from the other browsing data relating to the End User; for analytics, it is used only together with the browser user agent, as a keyed hash whose key is discarded within two days, to group an End User’s interactions into visits.
- In addition, in order to mitigate cross-border transfer risks, the architecture implements a server-side logical shield: for processing prompt text, the Callimacus back-end makes the server-to-server calls to the non-EU inference Sub-processors, whose servers record only the static IP address of Callimacus's European cloud and not the real IP address of the End User.
- Payment data in clear text: by default, the SDK does not collect payment data in clear text.

4. GEOLOCATION

Type	Features
Approximate geolocation (without IP)	Source: derived from non-personal signals (e.g. language settings, time zone, CDN patterns, browser approximations when configured without precision). Output: low-resolution area labels. Use: for non-invasive personalization (e.g. language, product range).
Physical geolocation (optional)	Where the Client requests activation of the geolocation service via Google Maps Platform, access to the device's precise GPS coordinates takes place only after the browser's system permission has been granted; in this case Google acts as an independent controller.

5. DURATION AND RETENTION

Duration of the "intent_sid" cookie: 30 (thirty) days by default (unless configured otherwise by the Client according to its business policies, or deleted earlier by the End User).

6. TRANSPARENCY, CONSENT AND BANNER

- Classification: intent_sid includes non-strictly-necessary components (personalization): it requires consent.
- Cookie notice: clearly state: name (intent_sid), standard default duration (30 days), purpose (semantic personalization), type of data involved and how to opt-out immediately.

7. PRIVACY ROLES AND ACCOUNTABILITY

Provision of the Platform on a SaaS basis:

Role	Party
Data Controller	The Client (company or consumer that owns the website)
Data Processor	Callimacus S.r.l.

8. SUMMARY LEGAL ASSESSMENT

Provided that the Client does not change the default masking configuration (para. 3.1), client-side capture of the interaction data linked to the intent_sid cookie takes place after the End User has given specific consent to the cookie.

9. USER INTERFACE AND RIGHTS

- Privacy preferences: panel for changing consent on every page; "Cookie settings" link.
- Immediate opt-out: opting out removes the intent_sid cookie and stops the collection.
- Data Subject rights: the Client must have a channel for exercising rights (DSR).

10. PROHIBITED AI PRACTICES AND MANDATORY RESTRICTIONS ON USE (AI ACT)

Activation of the intent_sid cookie, interaction with the algorithmic agents and prompt analysis are provided by Callimacus to Clients for the purposes described in this document and in the AI Act Report (Schedule 1 to the DPA), including browsing assistance and the personalization and optimization of the user experience.

Pursuant to Regulation (EU) 2024/1689 (AI Act), Callimacus does not carry out, and prohibits Clients under the Contract (T&C) from configuring, integrating or using the semantic data collected through the intent_sid cookie for, the following High-Risk or prohibited purposes:

Excluded purpose	Description
Credit Scoring & Financial Reliability	Assessment of the creditworthiness or solvency of natural persons.
Discriminatory Dynamic Pricing	Setting dynamic prices based on profiling of the End User's socio-economic, psychological or health vulnerabilities, age group, disability or psycho-physical conditions; the Platform has no technical features for dynamically changing or differentiating the price lists of the products and services displayed.
E-Recruitment & Personnel Selection	CV screening, candidate assessment or monitoring of work performance.
Insurance Risk Assessment	Risk assessment and premium setting for life and health insurance policies.
Emotion Recognition in the Workplace or in Education	Use of the agents' algorithmic inferences in school, academic or workplace settings.

Schedule 4 – List of Sub-processors – Client Version

CALLIMACUS S.R.L.

Service: provision of the Callimacus Platform on a SaaS basis

11.11.2026

Client version

SUB-PROCESSORS AUTHORIZED UNDER ARTICLE 5.1 OF THE DPA

Note. The following are not Sub-processors: Google Ireland Limited / Google LLC (Google Maps Platform), which acts as an independent controller and only if physical geolocation is enabled by the Client; Cohere Inc. / Cohere Technologies Inc. (Cohere), whose reranking model is used via Amazon Bedrock without Cohere receiving any Personal Data.

Company name	**Registered office**	**Processing activities performed**	**Processing details (purposes, categories of Personal Data, categories of Data Subjects, retention periods)**	**Processing locations**	**Safeguard mechanisms (if processing outside the EEA)**
Amazon Web Services EMEA SARL Amazon Web Services, Inc.	Luxembourg (Amazon Web Services EMEA SARL) USA (Amazon Web Services, Inc.)	Platform hosting: AWS Amplify and Amazon CloudFront for hosting the Client's website and for the distribution of the static assets of the SDK and of the front-end; AWS ECS Fargate cluster for core application logic, agents and the WAF security perimeter; Amazon Aurora and Amazon S3 for storing the Controller's data and files; Amazon S3 bucket for End User access logs; Amazon SES for sending to the Controller the messages End Users submit through the forms of its website and for sending verification codes to End Users; AWS WAF for network-level security monitoring. Amazon Bedrock for reordering search results by relevance (reranking) with the Cohere Rerank 3.5 model.	Purposes: hosting and provision of the Platform, security, reordering of search results. Data: session and interaction data, prompt content, access logs with IP address; contact details and messages End Users send through forms. Data Subjects: visitors and End Users of the Controller's website. Retention: for the duration of the Contract, subject to Article 9.	EU: Region eu-west-1 (Ireland); Region eu-central-1 (Frankfurt) for Amazon Bedrock; Amazon CloudFront edge locations worldwide for delivering the Client's website.	SCCs incorporated into the AWS DPA via the AWS Service Terms; DPF certification of Amazon Web Services, Inc.
Anthropic Ireland, Limited (EEA contracting entity) Anthropic, PBC	Ireland (Anthropic Ireland, Limited) USA (Anthropic, PBC)	Building and changing the Client's website through Anthropic's managed agents: analysis of the content of the Client's existing website, including screenshots, of the content provided by the Client and of the instructions of its Team Members; generation of the website's code and content.	Purposes: building and changing the Client's website. Data: content of the Client's existing website and content provided by the Client, including the Personal Data they contain; names,	USA.	SCCs Modules 2 and 3 (Anthropic DPA of 24.2.2025, §I.1).

Company name	Registered office	Processing activities performed	Processing details (purposes, categories of Personal Data, categories of Data Subjects, retention periods)	Processing locations	Safeguard mechanisms (if processing outside the EEA)
			instructions and attachments of the Client's Team Members. Data Subjects: natural persons mentioned in that content; the Client's Team Members. Retention: for the duration of the Contract, subject to Article 9.		
ClickHouse, Inc. (ClickHouse Cloud)	San Francisco (USA)	Storage of system logs, operational metrics, session telemetry and technical traces of AI processing, which contain the text of End Users' prompts and of the responses; persistence and analysis of metrics.	Purposes: storage and analysis of logs, metrics and telemetry. Data: system logs, operational metrics, session telemetry; technical traces of AI processing, including the text of End Users' prompts. Data Subjects: visitors and End Users of the Controller's website. Retention: for the duration of the Contract, subject to Article 9.	EU: selected Region; processing outside the Region only where reasonably necessary to provide the service or to comply with legal obligations (ClickHouse DPA, §6.1).	DPF certification (ClickHouse DPA of 10.4.2026, §6.5).
Datadog, Inc.	New York (USA)	Runtime application observability and security (App & API Protection / Application Security Management): logical inspection and monitoring of application threats, including Prompt Injection; log search indexes.	Purposes: application observability and security. Data: application and security logs, IP addresses, request content for threat detection purposes. Data Subjects: visitors and End	EU: EU1 site (Germany); possible remote support access from the USA.	SCCs Modules 2 and 3 (Datadog DPA, §10.1); DPF certification of Datadog, Inc.

Company name	Registered office	Processing activities performed	Processing details (purposes, categories of Personal Data, categories of Data Subjects, retention periods)	Processing locations	Safeguard mechanisms (if processing outside the EEA)
			Users of the Controller's website. Retention: security IP logs 90 days for suspicious requests; underlying traces 15 days.		
Groq UK Limited (EMEA contracting entity) Groq LLC	United Kingdom (Groq UK Limited) USA (Groq LLC)	Low-latency inference of open-architecture models, in a Zero Data Retention configuration, for back-end processing (interpretation of requests, reformulation of knowledge base queries, generation of responses, processing of display parameters on the front-end); Speech-to-Text transcription of voice input.	Purposes: processing of requests, generation of responses, transcription of voice input. Data: content of text and voice prompts. Data Subjects: visitors and End Users of the Controller's website. Retention: Zero Data Retention.	USA (GroqCloud).	SCCs Modules 2 and 3 (Groq DPA of 15.10.2025, §8.2).
OpenAI Ireland Ltd (EEA contracting entity) OpenAI OpCo, LLC	Ireland (OpenAI Ireland Ltd) San Francisco, USA (OpenAI OpCo, LLC)	Moderation of End Users' messages and voice interaction of the Client's Team Members with the Platform; the GPT models and embeddings are reached through OpenRouter (see the OpenRouter row).	Purposes: moderation, voice interaction, generation of responses and computation of embeddings. Data: content of text prompts; voice of Team Members. Data Subjects: visitors and End Users of the Controller's website; the Client's Team Members. Retention: for the duration of the Contract, subject to Article 9.	USA.	SCCs Modules 2 and 3 (OpenAI DPA of 1.1.2026).

Company name	Registered office	Processing activities performed	Processing details (purposes, categories of Personal Data, categories of Data Subjects, retention periods)	Processing locations	Safeguard mechanisms (if processing outside the EEA)
Pinecone Systems Inc.	USA	Vector database for storing and retrieving the embeddings of content and corporate knowledge.	Purposes: storage and retrieval of the Controller's knowledge base. Data: embeddings of the Controller's content and corporate knowledge, including any Personal Data contained therein. Data Subjects: any natural persons mentioned in the Controller's content. Retention: for the duration of the Contract, subject to Article 9.	EU: AWS eu-west-1 (Ireland).	SCCs Modules 2 and 3 (Pinecone DPA, §11.3); the DPF may replace the SCCs (§11.2).
OpenRouter, Inc.	USA	Routing of requests to the language and embedding models hosted by the providers listed in the next row.	Purposes: generation of responses, screening of End Users' text for Phantom, computation of embeddings. Data: text of End Users' prompts and conversation history (including text before redaction by Phantom), content of the Controller's website and knowledge base. Data Subjects: visitors and End Users of the Controller's website; natural persons mentioned in the Controller's content.	USA	SCCs (OpenRouter DPA).

Company name	Registered office	Processing activities performed	Processing details (purposes, categories of Personal Data, categories of Data Subjects, retention periods)	Processing locations	Safeguard mechanisms (if processing outside the EEA)
Model providers reached through OpenRouter		Google LLC / Google Cloud (Gemini models, on Vertex AI under Callimacus's own Google Cloud account or on Google AI Studio, for the default chat responses and for embeddings); Groq LLC (open-architecture models, including Phantom's redaction model); Cerebras Systems Inc. (open-architecture models); OpenAI OpCo, LLC and Microsoft Corporation – Azure OpenAI (GPT models and embeddings); TypeSafe AI, Inc. (models screening End Users' text for Phantom and composing and ranking responses).	Same data as OpenRouter	USA; EU for some Azure OpenAI deployments	SCCs; DPF for Microsoft Corporation and Google LLC.
Eleven Labs Inc.	USA	Speech synthesis of the responses of the Controller's website, where the voice feature is enabled.	Data: text of the responses read aloud. Data Subjects: visitors and End Users of the Controller's website.	USA	DPF; SCCs (ElevenLabs DPA).
LlamaIndex, Inc. (LlamaCloud)	USA	Parsing of documents the Client uploads, in formats the Platform does not parse itself.	Data: documents and the Personal Data they contain. Data Subjects: natural persons mentioned in the Controller's content.	USA	SCCs Modules 2 and 3 (LlamaIndex DPA).
Hugging Face, Inc.	USA	Inference endpoint dedicated to Callimacus in the AWS Region eu-west-1, reached over a private connection, computing sparse embeddings of the Controller's content and of End Users' prompts.	Data: text of the Controller's content and of End Users' prompts. Data Subjects: visitors and End Users of the Controller's website; natural persons mentioned in the Controller's content.	EU: AWS eu-west-1 (Ireland)	[to be confirmed]

Company name	Registered office	Processing activities performed	Processing details (purposes, categories of Personal Data, categories of Data Subjects, retention periods)	Processing locations	Safeguard mechanisms (if processing outside the EEA)
Cloudflare, Inc.	San Francisco (USA)	Browser Run: reading, rendering and capture of the public pages of the Client's existing website to build and change the Controller's website.	Data: content of the Client's existing website, including the Personal Data it contains. Data Subjects: natural persons mentioned on that website.	Global network	SCCs; DPF (Cloudflare DPA).
GitHub, Inc.	San Francisco (USA)	Storage and version control of the code and content of the Controller's website.	Data: content incorporated in the Controller's website, including the Personal Data it contains. Data Subjects: natural persons mentioned in that content.	USA	DPF; SCCs (GitHub DPA).