Privacy Notice

Callimacus S.r.l. · Version 2026-11-12 of 12 November 2026

PRIVACY NOTICE

CALLIMACUS S.R.L.

callimacus.ai website – Notice pursuant to Article 13 of Regulation (EU) 2016/679 (GDPR)

Last updated: 12 November 2026

1. INTRODUCTION

This notice describes the processing of personal data carried out through the **callimacus.ai** website (hereinafter, the "**Website**"), including by means of the artificial intelligence platform called "**Callimacus**" (hereinafter, the "**Platform**"), integrated into the Website to offer AI-assisted browsing.

For the purposes of this notice, "**user**" means any visitor to the Website, regardless of whether they actually interact with the AI assistant.

Information on the cookies and other tracking tools used by the Website and on how to give or withdraw consent is provided in the Cookie Policy published on the Website, to which reference is made.

2. CONTROLLER AND CONTACT DETAILS

Item	Details
Controller	Callimacus S.r.l., with registered office at Piazzetta dei Sapienti n. 1, Solomeo, 06073 Corciano (PG), Italy, VAT No. 03950820542 (hereinafter, the "Controller" or "Callimacus")
E-mail	privacy@callimacus.ai

3. HOW THE WEBSITE'S AI ASSISTANT WORKS

The Platform is a multi-agent artificial intelligence system that interprets the user's requests entered in the assistant's dialog bar (prompt bar), generates responses and adapts the Website's content and layout in real time. The AI assistant is used only at the user's choice, according to two distinct levels of consent:

- **consent to the use of artificial intelligence**, given through the dedicated banner (AI banner);
- **specific consent to personalization**, given through the cookie banner: activation of the "intent_sid" cookie for browsing personalization.

In accordance with Article 50(1) of Regulation (EU) 2024/1689 ("**AI Act**"), the user is informed, through a notice in the Website interface, that they are interacting with an artificial intelligence system.

The AI assistant and browsing personalization are reserved for users aged **14 or over**, the minimum age to give consent independently (Article 8 GDPR, Article 2-quinquies of Legislative Decree No. 196/2003 and Article 4(4) of Law No. 132/2025). Minors under the age of 14 must therefore not give consent or use the AI assistant. If it becomes aware that consent has been given by a minor under the age of 14, the Controller takes the necessary measures to delete the related data.

4. PURPOSES, DATA PROCESSED, LEGAL BASES AND NATURE OF THE PROVISION OF DATA

The following table indicates, for each purpose, the categories of personal data processed, the legal basis of the processing and whether the provision of data is mandatory or optional, as well as the consequences of any failure to provide the data.

Purpose	Data processed	Legal basis	Provision of data
a) AI-assisted browsing (interpretation of requests, generation of responses, adaptation of content and layout).	Text prompts, i.e. the text typed by the user in the assistant's dialog bar.	Consent (Article 6(1)(a) GDPR), given through the AI banner.	Optional: without consent, the AI assistant is not activated and the Website can still be browsed.
b) Personalization of the browsing experience and use of the Website.	Pseudonymous session identifier stored in a personalization cookie (in this regard, see the Cookie Policy of the Website), associated with: - statistical probability score associated with the user's interest (Intent Scoring); - urgency and sentiment indicators, derived on a transient basis from the writing style; - pages visited within the Website, time spent and click sequence in the active session; - browser type, operating system and device category.	Specific consent (Article 6(1)(a) GDPR), given through the cookie banner (in this regard, see the Cookie Policy of the Website).	Optional: without consent, assisted browsing remains limited to the current session, without personalization.
c) IT security of the Website and the Platform, including through a web application firewall (WAF), detection of cyber threats (for example, "prompt injection" attempts) and perimeter defense.	IP address, access and security logs, content of the requests made to the Platform.	Legitimate interest of the Controller in ensuring the security of its systems (Article 6(1)(f) GDPR).	Necessary: the data are collected automatically during browsing; without their processing, the Website cannot be browsed securely.
d) Statistical analysis and Business Intelligence (BI) on aggregated or anonymous data.	Browsing and interaction data relating to the Website and the AI assistant, used in aggregated or anonymous form. Statistics obtained through analytics cookies or other tracking tools are described in the Cookie Policy of the Website.	Consent of the user (Article 6(1)(a) GDPR), given through the cookie banner, for data collected through analytics cookies or other tracking tools (see the Cookie Policy of the Website). Legitimate interest of the Controller in knowing, in aggregated or anonymous form, how the Website and the Platform are used (Article 6(1)(f) GDPR), for data collected without the use of such tools.	Optional for data collected through analytics cookies or other tracking tools: without consent, such tools are not activated and the Website can still be browsed. For other data, not mandatory: the data are collected automatically during browsing and used in aggregated or anonymous form; the user may object to the processing (Article 21 GDPR), without consequences for the ability to browse the Website.

e) Handling of requests for information sent through the dedicated form or by writing to the Controller's contact details.	First and last name, e-mail address, company (optional) and information contained in the message.	Performance of pre-contractual measures taken at the request of the data subject (Article 6(1)(b) GDPR).	Necessary (except for optional fields): without personal data it is not possible to respond.
f) Handling of job applications sent through the dedicated form or by writing to the Controller's contact details, and of the resulting recruitment process, together with related activities.	First and last name, e-mail address, curriculum vitae and cover message, as well as any other information provided during the selection process (for example, personal details, contact details, educational and professional background, photograph). Any special categories of data, where provided by the data subject (for example, membership of protected categories).	Performance of pre-contractual measures taken at the request of the data subject (Article 6(1)(b) GDPR; Article 111-bis of Legislative Decree No. 196/2003). For any special categories of data: carrying out obligations and exercising specific rights in the field of employment law (Article 9(2)(b) GDPR).	Necessary: without the data it is not possible to handle the application and carry out the selection activities.
g) Compliance with legal obligations to which the Controller is subject, as well as with orders and measures of the authorities.	Data necessary to comply with the legal obligation (for example, contact details for communications required by law or by the authorities).	Legal obligation (Article 6(1)(c) GDPR).	Mandatory by law: without the data, the Controller cannot comply with legal obligations or, where the data are necessary, follow up on the data subject's requests.
h) Protection of rights (need to establish, exercise or defend a right in or out of court, or whenever the authorities exercise their functions).	Personal and contact details, as well as any other data necessary to protect rights (for example, data relating to any dispute).	Legitimate interest in protecting rights (Article 6(1)(f) GDPR). With regard to the processing of "special categories of data", the legal basis is also the need to establish, exercise or defend legal claims (Article 9(2)(f) GDPR). With regard to the processing of "judicial data", the legal basis is also the law (Article 10 GDPR and Article 2-octies of Legislative Decree No. 196/2003).	Necessary: the processing concerns data already held by the Controller; without it, the Controller could not establish, exercise or defend its rights.

The content of the prompts depends on what the user enters. Users are advised not to enter personal data, whether their own or relating to third parties, in the prompts.

Within the Platform, the user's full IP address is collected exclusively for security and cyber defense purposes and is processed separately from other browsing data, so as to make reconciliation with them impossible.

5. PROFILING AND AUTOMATED DECISION-MAKING

Only with specific consent to the personalization of the browsing experience and use of the Website (item (b) of the table in Section 4) does the Platform process the user's data by automated means to estimate their interest and adapt the content and layout of the Website accordingly. Urgency and sentiment indicators are transient inferences, used solely to calibrate the tone of the assistant's responses.

Such personalization concerns exclusively the content and presentation of the Website and does not involve decisions producing legal effects concerning the user or similarly significantly affecting them within the meaning of Article 22 GDPR. In particular, the data collected through the Platform are not used for creditworthiness assessment, recruitment, insurance risk assessment or emotion recognition in the workplace or in education.

The improvement of the Platform (self-learning) takes place exclusively on aggregated behavioral metrics and on abstract strings that have been anonymized in advance, without any modification of the weights of the language models.

6. PROCESSING METHODS AND SECURITY MEASURES

The data are processed mainly by electronic and telematic means, using logic strictly related to the stated purposes and through technical and organizational measures designed to ensure a level of security appropriate to the risk, pursuant to Article 32 GDPR, and to prevent the loss or destruction of the data, their unlawful or improper use and unauthorized access.

Such measures include, among others, encryption of communications, logical separation of data, minimization of the data transmitted to providers and systems for monitoring and controlling interactions with the AI assistant.

7. RECIPIENTS OF THE DATA

The data may be disclosed, to the extent necessary for the stated purposes, to the following parties:

- **authorized personnel** of the Controller (employees and collaborators), acting under its authority and on the basis of specific instructions;
- **providers** used by the Controller to operate the Website and the Platform (hosting and cloud infrastructure services, IT monitoring and security, log and metrics storage, databases, artificial intelligence language models), acting as **processors** pursuant to Article 28 GDPR;
- **consultants and professionals** (for example, lawyers), to the extent necessary to comply with legal obligations and to protect the Controller's rights (items (g) and (h) of the table in Section 4), acting as independent controllers or processors;
- **employment agencies and companies specializing in personnel search and selection**, solely for the handling of job applications (item (f) of the table in Section 4), acting as independent controllers;
- providers of statistical analysis and advertising services that place cookies or other tracking tools on the Website, acting as processors, independent controllers or joint controllers, as indicated in the Cookie Policy of the Website;
- **judicial authorities and other public authorities**, where required by law or for the establishment, exercise or defense of a right.

Personal data are not disseminated. The updated list of processors may be requested from the Controller at the contact details indicated in Section 2.

8. TRANSFER OF DATA OUTSIDE THE EUROPEAN ECONOMIC AREA

Some of the providers used by the Controller are established, or process the data, outside the European Economic Area, in particular in the United States and the United Kingdom. In such cases, the transfer takes place in compliance with Articles 44 et seq. GDPR, on the basis of an adequacy decision of the European Commission (for example, for US providers certified under the EU-U.S. Data Privacy Framework) or of the standard contractual clauses adopted by the European Commission with Decision (EU) 2021/914.

The data subject may obtain information on the safeguards adopted and a copy thereof by writing to the Controller at the contact details indicated in Section 2.

9. DATA RETENTION PERIODS

Purpose	Retention period
a) AI-assisted browsing	For the duration of the browsing session, without storing a user identifier. If consent is withdrawn, the data collected in the session are permanently discarded on the user's device. Prompts transmitted to the providers of the language models, acting as processors, are retained only for the time strictly necessary to process the request, within the limits set out in the agreements entered into with the Controller pursuant to Article 28 GDPR, and then deleted; some providers operate in a "Zero Data Retention" configuration.
b) Personalization of the browsing experience and use of the Website	6 (six) months, corresponding to the duration of the "intent_sid" cookie, unless the cookie is deleted earlier by the user. If consent is withdrawn, the cookie is removed and the data collected are permanently discarded on the user's device.
c) IT security	Security logs containing the IP address: 90 (ninety) days for suspicious requests and 15 (fifteen) days for the underlying traces. Other access and security logs: for the time strictly necessary for IT security purposes, after which they are deleted or anonymized, unless they need to be retained further to investigate security incidents or to protect rights (item (h)).
d) Statistical analysis and Business Intelligence (BI)	Personal data are processed only for the time necessary to aggregate or anonymize them. Anonymized data, as they do not constitute personal data, may be retained without time limits.
e) Handling of requests for information	6 (six) months from the completion of the handling of the request.
f) Handling of job applications	24 (twenty-four) months from the acquisition of the data by the Controller.
g) Compliance with legal obligations	For the period provided for by the specific legal provision and, failing that, for a maximum period of 10 (ten) years from the end of the calendar year in which the Controller fulfilled the obligation, in order to document and be able to demonstrate proper compliance.
h) Protection of rights	Until the conflict or dispute can be considered definitively settled, including any appeal proceedings.

Once the above periods have expired, the data are deleted or irreversibly anonymized.

10. DATA SUBJECT RIGHTS

By sending an e-mail to privacy@callimacus.ai, the data subject may exercise at any time the rights granted by data protection legislation (Articles 7, 15 et seq. GDPR), within the limits provided for by law; in particular, the right to:

- obtain **confirmation** as to whether or not personal data concerning them are being processed by the Controller (Article 15);
- **access** their personal data, know the purposes of the processing, the categories of data concerned and the recipients to whom they are disclosed, and obtain a copy in an intelligible form (Article 15);
- obtain the **rectification** of inaccurate data and the completion of incomplete data, without undue delay (Article 16);
- obtain the **erasure** of their data, without undue delay, in the cases provided for by law, including with regard to data collected online while they were a minor (Article 17);
- obtain the **restriction** of processing in the cases provided for by law (Article 18);
- request and receive, in a structured, commonly used and machine-readable format, the data provided to the Controller, and transmit them to another controller, where the processing is based on consent or on a contract and is carried out by automated means (so-called "**portability**", Article 20);
- **object** at any time, on grounds relating to their particular situation, to the processing of their personal data based on the Controller's legitimate interest (Article 21);

- **not** be subject to a **decision based solely on automated processing**, including profiling, which produces legal effects concerning them or similarly significantly affects them (Article 22);
- **withdraw** at any time **any consent** given, without affecting the lawfulness of processing based on consent before its withdrawal (Article 7(3)), including through the cookie preference management panel (see the Cookie Policy of the Website).

The exercise of rights is **free of charge and unrestricted**, except in the case of manifestly unfounded or excessive requests (Article 12(5) GDPR).

The data subject will receive a response from the Controller without undue delay and in any event within one month of receipt of the request, without prejudice to an extension of a further two months in cases of particular complexity or due to the number of requests; in such case, the Controller will send an interim communication within one month, stating the reasons for the delay. Where there are reasonable doubts concerning the identity of the requester, the Controller may request the information necessary to confirm it.

11. COMPLAINT TO THE SUPERVISORY AUTHORITY

If the data subject considers that the processing of their data infringes data protection legislation, they may lodge a complaint with the supervisory authority, which in Italy is the **Garante per la protezione dei dati personali** (www.garanteprivacy.it).

The complaint may also be lodged with a supervisory authority other than the Italian one, where it is the authority of the EU Member State of the data subject's habitual residence or place of work, or of the place of the alleged infringement (Article 77 GDPR).

12. CHANGES TO THIS NOTICE

The contents of this notice may change over time, in particular as a result of changes to the purposes and methods of the processing of personal data or to applicable legislation. The updated version is published on this page, indicating the date of its last update. In the event of significant changes, the Controller will notify data subjects by appropriate means.