



**Version: 11**

**Publish Date: 20th October 2026**

## **PARTIES**

This Agreement is between Customer and Claromentis. "Customer" is defined as the legal entity for which this agreement is being signed. If the agreement is not for a legal entity, then the "Customer" is the individual who accepts the terms.

## **JURISDICTIONAL APPLICABILITY**

This DPA contains provisions addressing multiple data protection regimes. Only the provisions applicable to Customer's jurisdiction shall apply:

- **Section 8 (United States Data Privacy Provisions)** applies only where Customer is subject to US Data Protection Laws.
- **Section 9 (UK and EU Data Privacy Provisions)** applies only where Customer is subject to UK GDPR or EU GDPR.
- **All other sections** apply universally to all Customers regardless of jurisdiction.

Where a Customer is not subject to a particular jurisdiction's laws, the provisions specific to that jurisdiction shall have no force or effect with respect to that Customer.

## **AGREED TERMS**

### **1. Definitions and interpretation**

The following definitions and rules of interpretation apply in this agreement.

#### **Definitions:**

**Data Protection Legislation:** (i) the Data Protection Act 2018 (DPA); (ii) the UK GDPR as defined in section 3(1) (as supplemented by section 205(4)) of the DPA (UK GDPR); (iii) EU GDPR (Regulation (EU) 2016/679); (iv) US Data Protection Laws (as defined below); and (v) any and all guidance and codes of practice issued by the relevant data protection supervisory authority (being, in the United Kingdom, the Information



Commissioner, or in the United States, applicable state attorneys general or federal authorities) and applicable to a party.

**US Data Protection Laws:** All applicable US federal and state privacy and data protection laws and regulations, including but not limited to: (i) California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA); (ii) Virginia Consumer Data Protection Act (VCDPA); (iii) Colorado Privacy Act (CPA); (iv) Connecticut Data Privacy Act (CTDPA); (v) Utah Consumer Privacy Act (UCPA); (vi) other applicable US state privacy laws; and (vii) any regulations, guidance, or codes of practice issued by relevant US supervisory authorities, in each case as amended, repealed, consolidated, or replaced from time to time.

**Data Subject:** as defined under Article 4 of the UK GDPR. Under US Data Protection Laws, includes "Consumer" as defined in applicable state laws.

**Controller:** The entity that determines the purposes and means of Processing Personal Data. Under EU/UK law, has the meaning given in the UK GDPR and EU GDPR. Under US Data Protection Laws, includes "Business" as defined in the CCPA and equivalent terms under other state laws. For purposes of this agreement, Controller means Customer.

**Processor:** The entity that processes Personal Data on behalf of the Controller. Under EU/UK law, has the meaning given in the UK GDPR and EU GDPR. Under US Data Protection Laws, includes "Service Provider" and "Contractor" as defined in the CCPA and equivalent terms under other state laws. For purposes of this agreement, Processor means Claromentis.

**Personal Data:** as defined under Article 4 of the UK GDPR, and includes "personal information," "personally identifiable information," or similar terms as defined under US Data Protection Laws.

**Processing, processes and process:** as defined under Article 4 of the UK GDPR, and includes equivalent terms under US Data Protection Laws.

**Personal Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Protected Data transmitted, stored or otherwise processed. Under US Data Protection Laws, includes "security incident," "data breach," or equivalent terms requiring notification under applicable law.

**Protected Data:** the Personal Data processed by Claromentis received from the Controller, or otherwise obtained in connection with the performance of the obligations of Claromentis under this agreement, the details of which are described in Annex A.

**Sale/Sell:** Has the meaning given in the CCPA and equivalent terms under other US Data Protection Laws.



**Share/Sharing:** Has the meaning given in the CCPA and equivalent terms under other US Data Protection Laws.

**Business Purpose:** Has the meaning given in the CCPA and equivalent terms under other US Data Protection Laws.

**Deidentified Data:** Data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, as defined under applicable US Data Protection Laws.

**Standard Contractual Clauses (SCCs):** the ICO's International Data Transfer Agreement for the transfer of personal data from the UK and/or the ICO's International Data Transfer Addendum to EU Commission Standard Contractual Clauses and/or the European Commission's Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 as set out in the Annex to Commission Implementing Decision (EU) 2021/914 and/or the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU.

**Intranet Software:** this refers to the 'Claromentis' software which is available via a web browser or mobile application.

- 1.1 This agreement is subject to the terms of the Customer Agreement and is incorporated into the Customer Agreement. Interpretations and defined terms set forth in the Customer Agreement apply to the interpretation of this agreement.
- 1.2 The Annexes form part of this agreement and will have effect as if set out in full in the body of this agreement. Any reference to this agreement includes the Annexes.
- 1.3 A reference to writing or written includes faxes and email. In the case of conflict or ambiguity between:
  - (a) any provision contained in the body of this agreement and any provision contained in the Annexes, the provision in the body of this agreement will prevail;
  - (b) the terms of any accompanying invoice or other documents annexed to this agreement and any provision contained in the Annexes, the provision contained in the Annexes will prevail;
  - (c) any of the provisions of this agreement and the provisions of the Customer Agreement, the provisions of this agreement will prevail; and
  - (d) any of the provisions of this agreement and any executed, the provisions of the executed SCC will prevail.

## 2. Scope of Processing and Compliance with Data Protection Legislation

Protected Data types and processing purposes



- 2.1 Both parties will comply with all applicable requirements of the Data Protection Legislation. This clause 2.1 is in addition to, and does not relieve, remove or replace, a party's obligations under the Data Protection Legislation.
- 2.2 The parties acknowledge that for the purposes of the Data Protection Legislation, Annex A sets out the scope, nature and purpose of processing by the Processor, the duration of the processing and the types of Protected Data and categories of Data Subject.
- 2.3 Without prejudice to the generality of clause 2.1, the Controller will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Protected Data to the Processor for the duration and purposes of this agreement.

### **3. Processor Obligations**

Without prejudice to the generality of clause 2.1, the Processor shall, in relation to any Protected Data processed in connection with the performance by the Processor of its obligations under this agreement:

- (a) process the Protected Data only on the written instructions of the Controller except where otherwise required by applicable law and in any such case the Processor shall promptly inform the Controller in writing of that legal requirement before performing the processing of the Protected Data, unless applicable law prevents it doing so on important grounds of public interest. The Processor shall immediately inform the Controller if the Processor believes any instruction relating to the Protected Data infringes or may infringe any Data Protection Legislation;
- (b) Claromentis will implement and maintain appropriate technical and organizational measures to protect the security, confidentiality, integrity, and availability of Customer Data and to prevent Security Incidents. Claromentis's current security measures are described at [claromentis.com/legal/security](https://claromentis.com/legal/security). The Customer is responsible for properly configuring the Claromentis Products and using the available security features to maintain an appropriate level of security for its Customer Data. Claromentis may update these security measures from time to time, as long as such changes do not materially decrease the overall security of the Cloud Products during a Subscription Term;
- (c) ensure that all personnel who have access to and/or process Protected Data are obliged to keep the Protected Data confidential;
- (d) assist the Controller, at the Controller's cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
- (e) notify the Controller without undue delay and in any event within forty-eight (48) hours of becoming aware of a Personal Data Breach;
- (f) at the written direction of the Controller, delete or return Personal Data and copies thereof to the Controller on termination of the agreement unless required by applicable law to store the Protected Data;



- (g) maintain complete and accurate records and information to demonstrate its compliance with this clause [3](#); and
- (h) make available to the Controller all information necessary to demonstrate compliance with Article 28 of the UK GDPR or EU GDPR (as applicable), and allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, subject to reasonable notice, confidentiality obligations and appropriate limitations to protect other customers and security. Information will first be provided by way of documentation, certifications and responses to written questionnaires. Where these are reasonably insufficient, on-site inspections are subject to: (A) no less than thirty (30) days' prior written notice; (B) normal business hours and minimal disruption to Claromentis's operations; (C) the Controller or its auditor agreeing in advance to reasonable confidentiality obligations; (D) no more than once per calendar year unless required by a supervisory authority or following a confirmed Personal Data Breach; and (E) the Controller bearing all reasonable costs associated with any on-site inspection.

#### **4. Sub-Processors and Subcontractors**

- 4.1 The Controller consents to the Processor appointing reputable third party domestic and international carriage partners as a third-party processor of Personal Data under this agreement. The Processor confirms that it has entered or (as the case may be) will enter with the third-party processor(s) into a written agreement incorporating terms which are substantially similar to those set out in clause 3. As between the Controller and the Processor, the Processor shall remain fully liable for all acts or omissions of any third-party processor appointed by it pursuant to this clause [4](#).
- 4.2 Claromentis maintains a list of the sub-processors currently instructed by the Processor at the following link: [www.claromentis.com/legal/sub-processors](http://www.claromentis.com/legal/sub-processors) The list includes details of each sub-processor's services, location, and data categories processed.
- 4.3 Claromentis will give the Controller at least thirty (30) days' prior notice by email of any intended addition or replacement of a sub-processor. The Controller may object on reasonable data protection grounds within that period, and the parties will discuss the objection in good faith. If the objection cannot be resolved, the Controller may terminate the affected Services on written notice, and Claromentis will refund any prepaid Fees for the period after termination.

#### **5. Term and Termination**

- 5.1 This agreement will immediately take effect upon entering into the Customer Agreement .
- 5.2 The provisions of this agreement shall survive the term of this agreement and the Customer Agreement , and in order to protect Protected Data shall remain in full force and effect.



## 6. Notices

- 6.1 Any notice or other communication given to a party under or in connection with this agreement must be in writing and shall be:
- (a) delivered by hand or by recorded delivery service at its registered office; or
  - (b) sent by email to [data-protection@claromentis.com](mailto:data-protection@claromentis.com) and [sales@claromentis.com](mailto:sales@claromentis.com) for Claromentis, and to the Customer's notice email address set out in the Order Form or otherwise notified in writing
- 6.2 Any notice shall be deemed to have been received:
- (a) if delivered by hand, at the time the notice is left at the proper address;
  - (b) if sent by recorded delivery at the time and date registered by the recorded delivery service; or
  - (c) if sent by email, on the next business day after transmission, provided always that no error message, out-of-office or other automated reply, bounce-back, or other notification of a failure of or delay to transmission is received by the party sending such notice within forty-eight (48) hours of attempted transmission.
- 6.3 Clause 6.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

## 7. Data Return and Deletion

Upon termination or expiry of this agreement, the Processor shall, at the Controller's written direction and within thirty (30) days of such direction and securely delete or destroy all Protected Data. The Processor may retain Protected Data to the extent required by applicable law, provided that the Processor shall:

- (A) notify the Controller in writing of any such legal requirement to retain;
- (B) continue to ensure the confidentiality and security of all such Protected Data;
- (C) only process such Protected Data as necessary to comply with the legal requirement; and
- (D) delete such Protected Data when the legal requirement ceases to apply.

## 8. United States Data Privacy Provisions

### 8.1 Roles of the Parties:

For purposes of applicable US Data Protection Laws:



- Customer is a “Business” or “Controller”
- Claromentis is a “Service Provider” and/or “Processor”

Claromentis shall process Personal Data solely:

- for the purpose of performing the Services,
- in accordance with the Customer Agreement and this DPA,
- and as otherwise permitted by applicable US Data Protection Laws.

## **8.2 No Sale or Sharing of Personal Data**

Claromentis shall:

- Not sell Personal Data;
- Not share Personal Data for cross-context behavioural advertising;
- Not retain, use, or disclose Personal Data for any purpose other than performing the Services;
- Not combine Personal Data with personal data received from other sources except as permitted under applicable US Data Protection Laws.

## **8.3 Consumer Rights Assistance**

Claromentis shall:

- Provide reasonable assistance to Customer to enable Customer to respond to consumer rights requests under US Data Protection Laws (including access, deletion, correction, portability, and opt-out rights);
- Notify Customer if it receives a request directly from a consumer relating to Customer Personal Data.

## **8.4 Sub-Processors (Service Providers)**

Claromentis shall:

- Impose contractual obligations on Sub-processors that are no less protective than those set out in this DPA;
- Remain liable for Sub-processor compliance as required by applicable US Data Protection Laws.

## **8.5 Audits (CPRA Requirement)**

Claromentis shall make available to Customer information reasonably necessary to demonstrate compliance with this Section, including by responding to written questionnaires and providing relevant documentation upon reasonable written request.



Where documentation review and questionnaire-based assessment are insufficient to satisfy the Customer's compliance obligations under applicable US Data Protection Laws, Claromentis shall allow for and contribute to reasonable on-site assessments or inspections, subject to the following conditions:

- (A) the Customer provides no less than thirty (30) days' prior written notice;
- (B) any assessment is conducted during normal business hours and in a manner that minimises disruption to Claromentis's operations;
- (C) the Customer (or any appointed third party auditor) agrees in advance to reasonable confidentiality obligations;
- (D) assessments are conducted no more than once per calendar year unless required by applicable law or following a confirmed Personal Data Breach; and
- (E) the Customer bears all reasonable costs associated with any on-site assessment.

## **8.6 Applicability of United States Data Protection Laws**

**The provisions of this Agreement relating to United States Data Protection Laws apply only to Customers subject to those laws. They do not apply to Customers outside the United States.**

Where United States Data Protection Laws apply and conflict with other provisions of this Agreement, the US-specific provisions will prevail to the extent of that conflict.

## **9. UK and EU Data Privacy Provisions**

Claromentis will not transfer any Protected Data outside of the United Kingdom (for Customers subject to the UK GDPR) or the European Economic Area (for Customers subject to the EU GDPR) unless the transfer is made to an adequate jurisdiction (within the meaning of Article 45(1) of the UK GDPR) or prior written consent of the Controller has been obtained and the following conditions are fulfilled:

- (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer;
- (ii) the Data Subject has enforceable rights and effective legal remedies;
- (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Protected Data that is transferred; and
- (iv) the Processor complies with reasonable instructions notified to it in advance by the Controller with respect to the processing of the Protected Data.



The Controller consents to transfers of Protected Data to the sub-processors listed at [www.claromentis.com/legal/sub-processors](http://www.claromentis.com/legal/sub-processors), provided such transfers are made on the basis of adequacy regulations or appropriate safeguards under Article 46 of the UK GDPR or EU GDPR (as applicable).

**This section 9 applies to Customers subject to the UK GDPR or the EU GDPR.**

Where UK or EU Data Protection Laws apply and conflict with other provisions of this Agreement, the UK and EU-specific provisions will prevail to the extent of that conflict.

## 9.1 AI Data Processing Regions

Claromentis uses artificial intelligence features (such as Vertex AI/Gemini APIs) for certain optional features within the Services. The geographic region where AI requests are processed is as follows:

- UK-hosted instances: AI processing is conducted via Google's EU endpoint (as of version 10.10.0 and 11.4.0). Previously, UK-hosted AI processing used Google's UK endpoint; however, due to changes in Google's regional model availability, UK-hosted AI processing has been moved to the EU endpoint.
- EU-hosted instances: AI processing is conducted via Google's EU endpoint.
- US-hosted instances: AI processing is conducted via Google's US endpoint.

Your core data and records remain hosted in your designated geographic region. Specific regions are used under the hood for vector embedding generation for search queries and document indexing, as that underlying model does not support broader jurisdictional regional boundaries.

AI features are optional and can be enabled or disabled at any time

## Annex A - Description of Processing

### Subject matter of processing:

Claromentis will process personal data to provide our software and product related support in accordance with the Customer Agreement and this DPA. The nature of this processing, including collection, structuring, storage, and transmission, is as described in Annex A and other relevant documentation.

### Duration of Processing:

For the duration of this Agreement.

### Nature of Processing:



We process personal information by hosting and accessing the controllers intranet site in order to deploy, maintain and support intranet software. Where enabled by the Controller, this processing may also include the operation of AI-assisted features to enable Authorised Users to query and retrieve information from the Controller's intranet content and document repository, as described in section 9.1.

### **Personal Data Categories:**

The data categories are unknown and it is the responsibility of the controller to decide what personal data categories are uploaded to the intranet software. It's possible that the personal data categories could include personal details, family details, lifestyle and social circumstances, goods and services, employment and education details, financial details, and any other personal details that data subjects may choose to share within the platform, including prompts and queries submitted through AI-assisted features, where enabled by the Controller.

### **Data Subject Types:**

The data subjects are unknown and it is the responsibility of the controller to decide the nature of the personal data that is uploaded to the intranet software. Its likely that the personal data subject types include the controller's clients, employees, suppliers and individuals.

**Sensitive data transferred:** The Customer is solely responsible for determining and controlling any Sensitive Data it or its Users upload to the Cloud Products. This includes special categories of personal data, as defined by applicable laws, such as data concerning racial or ethnic origin, health information, or criminal convictions.

**Transfers to Sub-processors:** Claromentis will transfer Customer Personal Data to Sub-processors as permitted in Section 4 (Sub-processors & Subcontractors).

**Prohibited Activities Confirmation:** Provider will not Sell or Share Personal Data, will not process Personal Data for purposes other than providing services to Customer, will not retain Personal Data beyond 30 days after termination, and will not combine Personal Data with data from other sources except for Business Purposes. Prompts and content submitted through AI-assisted features are not used by Claromentis to train or improve AI models, and are processed by Google under terms prohibiting their use to train or fine-tune Google's models without permission. To improve performance, Google may temporarily cache prompts and responses in memory for up to 24 hours within the processing region described in section 9.1, after which they are automatically discarded.