# Data Processing Agreement

Version: 5
Date Last Review: 10th March 2025

## BACKGROUND

To ensure compliance with the Data Protection Legislation, this Data Processing Agreement sets out the terms of how we will process the personal data that you pass to us. For the purposes of us providing our services, your company is acting as the data controller (**Controller**) and Claromentis is acting as the data processor (**Claromentis** or **Processor**).

Where we have entered into a Perpetual Licence Agreement or a Software as a Service Agreement this will be referred to throughout this document as the Master Agreement.

### AGREED TERMS

1.      Definitions and interpretation

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

1.1.    Definitions:

        **Data Subject:** as defined under Article 4 of the UK GDPR.

        **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**); and (iii) any and all guidance and codes of practice issued by the relevant data protection supervisory authority (being, in the United Kingdom, the Information Commissioner) and applicable to a party.

        **Personal Data:** as defined under Article 4 of the UK GDPR.

        **Processing, processes and process:** as defined under Article 4 of the UK GDPR.

**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.

**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.

**Standard Contractual Clauses (SCCs)**, means 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.

1.2.  This agreement is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this agreement.

1.3.  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.

1.4.  A reference to writing or written includes faxes and email.

1.5.  In the case of conflict or ambiguity between:

1.5.1.  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;

1.5.2.  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;

1.5.3.  any of the provisions of this agreement and the provisions of the Master Agreement, the provisions of this agreement will prevail; and

1.5.4.  any of the provisions of this agreement and any executed, the provisions of the executed SCC will prevail.

2.    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

3.1.  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:

3.1.1.   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;

3.1.2.   ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Protected Data and against accidental loss or destruction of, or damage to, Protected Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Protected Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Protected Data can be restored in a timely manner after an incident,

and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

3.1.3. ensure that all personnel who have access to and/or process Protected Data are obliged to keep the Protected Data confidential;

**3.1.4.** not transfer any Protected Data outside of the European Economic Area 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:

(a) the Controller or the Processor has provided appropriate safeguards in relation to the transfer;

(b) the Data Subject has enforceable rights and effective legal remedies;

(c) 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

(d) the Processor complies with reasonable instructions notified to it in advance by the Controller with respect to the processing of the Protected Data;

3.1.5. 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;

3.1.6. notify the Controller without undue delay on becoming aware of a Personal Data Breach;

3.1.7. 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; and

3.1.8. maintain complete and accurate records and information to demonstrate its compliance with this clause 3.1.

4.      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 3.1. 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.    Annex C contains details of the sub-processors or class of sub-processors instructed currently by the Processor.

5.      Term and termination

5.1.    This agreement will immediately take effect upon entering into the Master Agreement.

5.2.    The provisions of this agreement shall survive the term of this agreement and the Master Agreement, and in order to protect Protected Data shall remain in full force and effect.

6.      Notice

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:

    6.1.1.    delivered by hand or by recorded delivery service at its registered office; or

    6.1.2.    sent by email to the following addresses (or an address substituted in writing by the party to be served in accordance with this clause 6):

        (a)    Processor:

        (b)    Controller:

    6.1.3.    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.

6.2.    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.

Please confirm acceptance by signing below.  The terms of this agreement shall apply from the date of this      Master Agreement.

For the Controller:

Name:

Title:

Company Name:

Signed:

Date:

For the Processor:

Name: Will Emmerson

Title: Chief Information Officer

Company Name: Claromentis Ltd

Signed:

Date:

# ANNEX A - Personal Data Processing Purposes and Details

## Subject matter of processing:

We process personal information to enable us to provide web-based intranet software to the controller.

## Duration of Processing:

For the duration of this Agreement.

## Nature of Processing:

Master Agreement

The nature of processing shall be as is instructed by the Controller and as is reasonably necessary in accordance with the terms of the Master Agreement.

## 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.

## Data Subject Types:

The data subject types are Controller staff.  It is the responsibility of the Controller to decide what personal data is uploaded to the intranet software.

## ANNEX B – Security Measures

- Suppliers - Checked that security standards are met as part of a supplier review/security policy - this includes checking for ISO 27001, SOC2 or the equivalent security controls.
- Encryption is used for all customer data stored within the Claromentis SaaS platform - Data is encrypted In Use, At Rest and In Transit.
- Firewalls - Access control lists are in place for any externally facing systems
- Penetration testing - Carried out on an annual basis.
- Vulnerability scanning - The cloud infrastructure is scanned on a regular basis to check for any vulnerabilities.
- Patch Management  - Systems are patched according to the standards set out in our Information Security Policy.
- Product/Development - We have Secure Development standards that are clearly defined and shared with all team members.

# ANNEX C – Subcontractors

The subcontractors detailed below have been approved as third-party sub-processors by the Controller.

| Name of sub-processor | Jurisdiction in which the sub-processor is located | Jurisdiction in which the sub-processing takes place | Processing taking place |
|---|---|---|---|
| Google Cloud | USA | Europe (Frankfurt) | Google provides Cloud Hosting / Cloud Infrastructure which is operated on a shared responsibility model between Google and Claromentis. The data is processed and sits at rest within the region specified to the left. |
| SendGrid | USA | USA (same region for all customers - it can be disabled and you can your own SMTP / mail relay if required) | SendGrid is a transactional email delivery service. It's used to send out email notifications from Claromentis to the end user(s). |

<u>Claromentis (Processor)</u>

Company Name:     Claromentis Limited                                    Name of signatory: Will Emmerson
Title:   CIO
Date:
Signature:

<u>Customer (Controller)</u>

Company Name:
Name of signatory:
Title:
Date:
Signature: