Primo Data Processing Addendum

Version Number	2026.5
Review Date	May 11, 2026

This Data Processing Addendum (this "**Addendum**") supplements and forms part of the Terms and Conditions between the Customer and the Provider (the "**Agreement**"). Except as modified below, the terms of the Agreement shall remain in full force and effect. If there is a conflict between the Agreement and this Addendum, the terms of this Addendum will prevail. For the avoidance of doubt, this Addendum is effective as at the Effective Date of the Agreement and will remain in effect until termination of the Agreement; or the last Processing of Customer Personal Data carried out by or on behalf of the Customer under the Agreement.

1. Definitions

In this Addendum, the following words and expressions have the following meanings:

"Customer Personal Data" means Personal Data Processed by the Provider as Processor on behalf of the Customer pursuant to the performance of the Agreement.

"Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach", "Supervisory Authority" and **"Processing"** all have the meanings given to those terms in Data Protection Laws (and related terms such as "Process", "Processes" and "Processed" shall have corresponding meanings); and

"Data Protection Laws" means all laws and regulations relating to data protection and privacy as applicable to the Parties and/or to the Processing of Personal Data under this Agreement, including without limitation, the EU General Data Protection Regulation 2016/679 ("GDPR"), the GDPR in such form as incorporated into the laws of the United Kingdom ("UK GDPR"), the Data Protection Act 2018, and any associated implementing legislation and

regulations, in each case, as in force and applicable, and as amended, supplemented or replaced from time to time.

“Sub-Processor” means another Processor engaged by the Provider for carrying out Processing activities in respect of Customer Personal Data.

2. Data Processing Details and Compliance

1. The Parties acknowledge that in respect of Customer Personal Data, the Provider is a Processor Processing Personal Data on behalf of the Customer as Controller. Each Party shall comply with its obligations under Data Protection Laws as relates to Customer Personal Data.
2. Details of Customer Personal Data Processed by Provider under this Agreement are as follows:
    a. **Subject Matter, Nature and Purpose of Processing**. The Provider’s provision of the Services under this Agreement. In particular, providing the Customer with access to the Provider’s IT Operations platform.
    b. **Duration of Processing**. Processing of Customer Personal Data by the Provider shall be for the term of this Agreement and in accordance with the Provider’s retention obligations under this Agreement and Addendum, provided that Customer Personal Data shall not be Processed for longer than is necessary for the purpose for which it was collected or is being Processed (except where a statutory exception applies).
    c. **Personal Data in Scope.** Names, Communication details (Email, Phone number, etc.), Contact details, Job role; Login data; Profile image; Technical details (Device information, IP addresses, cookies, etc.)
    d. **Category of Data Subjects**. Customer personnel (employee, contractors, etc)

3. Data Processing Instructions

1. The Provider shall Process Customer Personal Data only on the written instructions of the Customer (including as set out in this Agreement) unless the Provider is required to otherwise Process Customer Personal Data by

applicable laws. The Provider is hereby instructed to Process Customer Personal Data for the purposes of providing the Services. In the event the Provider is required by applicable laws to Process Customer Personal Data other than in accordance with the Customer's instructions, prior to any such Processing and to the extent permitted by applicable laws, the Provider shall notify the Customer in writing of that legal requirement prior to Processing Customer Personal Data.

2. The Provider shall promptly inform the Customer if the Provider becomes aware of a written instruction given by the Customer under this Clause 3 that, in the Provider's reasonable opinion, infringes Data Protection Laws.

4. Provider Personnel and Sub-Processors

Company	Location	Type	DPA
AWS	EU	Cloud provider	Link
Datadog	EU	Observability platform	Link
MongoDB Cloud	EU	Cloud Database	Link
Plain	EU	Support tool	Link
Clerk	US	User management	Link
Kombo	EU	HR API integration tool	Link
Hubspot	EU	CRM	Link
PostHog	EU	Product Analytics	Link
Anthropic	US	LLM	Link
OpenAI	US	LLM	Link

1. The Provider shall ensure that all Provider personnel authorized to Process Customer Personal Data are either subject to binding written contractual obligations or statutory obligations to keep Customer Personal Data confidential.
2. The Customer authorizes the Provider to engage (including the disclosure of Customer Personal Data under this Agreement to such Sub-Processors) the Sub-Processors included in the following list ("Sub-Processor List"):
3. The Provider shall keep the Sub-Processor List updated and notify Customers of changes to the list.

4. Sub-Processor Change Notification**:** The Provider shall inform the Customer in writing at least 30 days before adding or replacing any Sub-Processor. Changes within an already approved category of Sub-Processors require only notification without objection rights, unless such change is reasonably likely to materially reduce the level of protection of Customer Personal Data (in which case the Customer shall have the right to object on legitimate compliance grounds within 10 business days following notification). For the addition of new categories, the Customer has the right to object on legitimate compliance grounds within 10 business days following notification. In case of a valid objection, the parties will seek an alternative solution within 30 days, failing which either party may terminate the contract.
5. LLM Sub-Processors - Training Opt-Out Guarantee**:** The Provider guarantees that no Customer Personal Data is used to train Large Language Models (LLMs). The Provider has contractual clauses with LLM Sub-Processors (Anthropic and OpenAI) explicitly prohibiting the use of data for model training. Customer data processed through LLM APIs is not retained beyond 30 days (for abuse/monitoring purposes only) and is automatically deleted thereafter.
6. Data Retention for LLM Processing: Data processed by LLM Sub-Processors is deleted within a maximum of 30 days and is not used to train or improve AI models.

5. Transfers

1. The Provider shall not transfer Customer Personal Data to any party in a country not deemed adequate for the transfer of Personal Data by the European Commission (for transfer concerning the EEA) and the equivalent UK authority (for transfers concerning the UK), including permitting access to Customer Personal Data from any party in such countries, without the prior written consent of the Customer, unless:
    a. the transfer/access is to a Sub-Processor included in the Sub-Processor List or appointed in accordance with Clause 4 of this Addendum; and
    b. the transfer/access is in compliance with Data Protection Laws (including having in place appropriate transfer safeguards as applicable).

2. Legal Instruments for International Transfers**:** For transfers to the United States (notably LLM Sub-Processors Anthropic and OpenAI), the Provider has implemented the European Commission's Standard Contractual Clauses (SCCs) 2021. In addition, the Provider has conducted Transfer Impact Assessments (TIA) and implemented supplementary measures including: (a) encryption of data in transit (TLS 1.3), (b) pseudonymization where possible before transmission, (c) data minimization principles, (d) contractual prohibition of access by US authorities except under legal obligation, and (e) notification commitment in case of government access requests.

6. Security and Personal Data Breach Notification

1. The Provider shall implement and maintain appropriate technical and organizational measures in relation to the Processing of Customer Personal Data to ensure a level of security appropriate to the risks which may occur as a result of Processing Customer Personal Data, and in particular the risks of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.
2. Technical Security Measures: The Provider implements the following technical measures:
    a. Encryption**:** Data at rest is encrypted using AES256-CBC on MongoDB Atlas; data in transit uses TLS 1.2 minimum (HTTPS systematic); secrets are managed via AWS Secrets Manager.
    b. Access Controls: Role-Based Access Control (RBAC) on AWS; principle of "need-to-know" with access limited to authorized developers only; bearer tokens and IP filtering for internal services; Clerk authentication (login/password + Google ID) for Cockpit; VPC to isolate internal services.
    c. Infrastructure: Hosting exclusively on AWS Paris region (eu-west-3); MongoDB Atlas on dedicated (non-shared) instance; BFF (Backend for Frontend) architecture to mask GraphQL schema.
    d. Endpoint Security: Mandatory MDM on all Primo devices (disk encryption, firewall, auto-lock); EDR (Sentinel One) deployed via MDM on all computers; remote wipe/lock enabled.

e. Monitoring and Detection: Regular vulnerability assessments (partnership with Bastion.tech); annual penetration testing as part of SOC2; access and activity logs.

3. Organizational Security Measures: The Provider maintains:
    a. Certifications: SOC 2 Type II certified (2024 and 2025); annual security audits.
    b. Governance: Privacy contact: Benoît Bourdel, Chief Technology Officer (benoit.bourdel@getprimo.com), who is Primo's internal owner for data protection matters; documented security policies; ongoing team training on security and GDPR.
    c. Incident Management: Personal Data Breach notification procedures (within 72 hours); dedicated security contact point.
4. The Provider shall notify the Customer without undue delay on becoming aware of a Personal Data Breach and provide the Customer with details of the Personal Data Breach as required under Data Protection Laws. To the extent available, these details shall include:
    a. the nature of the Personal Data Breach, including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Customer Personal Data records concerned
    b. the name and contact details of the data protection officer or other contact point of the Provider, where more information can be obtained
    c. description of the likely consequences of the Personal Data Breach; and
    d. description of the remedial actions taken or proposed to be taken to mitigate the effects and minimise any damage resulting from the Personal Data Breach.

7. Assistance

1. To the extent related to its Processing of Customer Personal Data (taking into account the nature of Processing and the information available to the Provider), the Provider shall promptly provide the Customer with reasonable assistance:
    a. using appropriate technical and organizational measures, in complying with any requests received from Data Subjects of Customer Personal

Data exercising Data Subject rights under Data Protection Laws;

b. to enable the Customer to conduct data protection impact assessments and consultations with (or notifications to) a relevant Supervisory Authority where the Customer is required to do so under Data Protection Laws, in connection with data protection impact assessments; and

c. in complying with its obligation to implement and maintain appropriate technical and organizational security measures to protect Customer Personal Data.

8. Deletion or Return of Data

1. The Provider shall, at the choice of the Customer delete or return all Customer Personal Data to the Customer once Processing by the Provider of any Customer Personal Data is no longer required for the purposes of this Agreement, and delete all existing copies unless required by applicable laws to store Customer Personal Data.

9. Information Requests and Audits

1. The Provider shall, on request from the Customer, make available to the Customer all information necessary to demonstrate the Provider's compliance with its obligations under this Agreement. The Provider shall allow for audits (including inspections) conducted by the Customer or the Customer's designated auditor on reasonable prior written notice, for the purpose of demonstrating the Provider's compliance with its obligations under this Agreement. For the avoidance of doubt such audits shall be limited to once per calendar year. Any additional audit under this Clause 9.1 (in excess of the once per calendar year limitation) shall be at the cost of the Customer, and the Provider may charge the Customer at its standard time-based charging rates for any work performed by the Provider at the request of the Customer pursuant to this Clause 9.1.
2. The Provider's obligations under Clause 9.1 of this Addendum are subject to the Customer:

   a. giving the Provider reasonable prior notice of such information requests, audits and/or inspections being required by the Customer;

b. ensuring that all information obtained or generated by the Customer or its auditor(s) in connection with such information requests, inspections and audits is kept strictly confidential (save for disclosure to a Supervisory Authority or as otherwise required by applicable laws); and

c. ensuring that such audit or inspection is undertaken during normal business hours, with, so far as reasonably practicable, minimal disruption to the Provider's business and the business of other customers of the Provider.