Maestro data processing agreement

Data processing agreement · Draft · 27 November 2026

Enterprise version of Schedule 4 of the Maestro Terms of Service v1.1; it prevails over Schedule 4 where the order form says so (Schedule 4, paragraph 1.2). Template for legal review before use. Square-bracket items [●] are filled per customer. Written under UK GDPR and the Data Protection Act 2018, with EU GDPR where the customer is in the EU.

Parties. (1) [Customer legal name], [registered address], company no. [●] (the **Customer**, controller); (2) Promethean Systems Ltd, registered in England and Wales, company no. 16774853, ICO registration CSN9976644 (**Promethean**, processor). This agreement forms part of the Maestro Terms of Service v1.1 and the order form between the parties dated [●] (together the **MSA**).

1. Definitions

Terms such as **controller**, **processor**, **personal data**, **personal data breach**, **data subject** and **processing** have the meanings in the UK GDPR (and, where it applies, the EU GDPR) (together, **Data Protection Law**). **Customer Personal Data** means personal data processed by Promethean on the Customer's behalf in providing the Maestro services under the MSA. **Subprocessor** means any third party Promethean engages to process Customer Personal Data.

2. Roles and scope

2.1 The Customer is the controller and Promethean is the processor of Customer Personal Data. Where the Customer is itself a processor for its own clients, Promethean acts as its sub-processor and the Customer confirms it has authority to appoint Promethean.

2.2 The subject matter, duration, nature and purpose of processing, the types of personal data and the categories of data subjects are set out in Annex 1.

2.3 Promethean is a controller only of account, billing and service-security data it needs to run its business, as described in its privacy policy.

3. Instructions

3.1 Promethean processes Customer Personal Data only on the Customer's documented instructions, which are this agreement, the MSA, the order form and the Customer's configuration and use of Maestro (including the workflows, integrations and approval policies it sets up).

3.2 Promethean will tell the Customer promptly if, in its opinion, an instruction breaches Data Protection Law, and may suspend that processing until the instruction is confirmed or changed.

3.3 Promethean will not use Customer Personal Data or other customer content to train, fine-tune or evaluate any AI model, its own or anyone else's, unless the Customer agrees in writing.

3.4 Promethean will not sell Customer Personal Data or use it for its own purposes.

4. Confidentiality

Promethean ensures that everyone it authorises to process Customer Personal Data is bound by a duty of confidentiality and has access only as far as their role needs.

5. Security

5.1 Promethean implements the technical and organisational measures in Annex 2, which are designed to give a level of security appropriate to the risk, as required by Article 32.

5.2 Promethean may update those measures over time, provided the overall level of protection is not reduced.

6. Subprocessors

6.1 The Customer gives general authorisation for Promethean to use the Subprocessors listed in Annex 3.

6.2 Promethean will give the Customer at least [30] days' written notice of any new or replacement Subprocessor. The Customer may object on reasonable data protection grounds within that period; the parties will then discuss the objection in good faith, and if they cannot resolve it the Customer may terminate the affected service without penalty and receive a pro-rata refund of prepaid fees.

6.3 Promethean imposes on each Subprocessor, by written contract, data protection obligations no less protective than those in this agreement, and remains liable to the Customer for each Subprocessor's performance.

7. Data subject rights

7.1 Promethean will pass to the Customer, within [5] business days, any request it receives from a data subject about Customer Personal Data, and will not answer it except on the Customer's instructions.

7.2 Taking into account the nature of the processing, Promethean will help the Customer, by appropriate technical and organisational measures, to respond to requests to exercise data subject rights.

8. Personal data breaches

8.1 Promethean will notify the Customer without undue delay, and in any case within [24] hours, after becoming aware of a personal data breach affecting Customer Personal Data.

8.2 The notice will describe, as far as then known, the nature of the breach, the categories and approximate numbers of data subjects and records concerned, the likely consequences and the measures taken or proposed. Promethean will update the Customer as more becomes known and provide a written root-cause and remediation report.

8.3 Promethean will not notify regulators or data subjects about a breach of Customer Personal Data on the Customer's behalf unless the Customer instructs it or the law requires it.

9. Assistance

Promethean will give the Customer reasonable help with data protection impact assessments, prior consultations with a supervisory authority and the Customer's other Article 32 to 36 obligations, as far as they concern Promethean's processing. Help beyond what is reasonable may be charged at the rates in the order form.

10. International transfers

10.1 Customer Personal Data is stored in the region stated in the order form (by default the EU, AWS Stockholm). AI processing runs on rented GPU servers operated by Promethean, in the locations set out in Annex 3; document parsing and integrations are processed in the United States as set out in Annex 3.

10.2 Promethean will not transfer Customer Personal Data outside the UK or the EEA except under an adequacy decision or the transfer mechanisms in Annex 4, and only for the services listed in Annex 3.

11. Audits

11.1 Promethean will make available to the Customer the information reasonably needed to show compliance with this agreement, including its current security documentation and any independent test or certification reports it holds.

11.2 The Customer, or an independent auditor bound by confidentiality, may audit Promethean's compliance once a year on [30] days' notice, during business hours and without disrupting other customers, and at any time after a personal data breach or where a supervisory authority requires it. Each party bears its own costs, unless the audit shows a material breach by Promethean.

12. Return and deletion

When the services end, Promethean will, at the Customer's choice, return Customer Personal Data in a common machine-readable format and then delete it, or delete it, within 90 days, and confirm deletion in writing. Promethean may keep copies only where the law requires it, and then only for as long as the law requires, under continued confidentiality.

13. Liability, order of precedence and term

13.1 Each party's liability under this agreement is subject to the limits in the MSA [except as agreed in the order form].

13.2 If this agreement conflicts with the MSA on the processing of personal data, this agreement prevails.

13.3 This agreement lasts for as long as Promethean processes Customer Personal Data. Clauses 4, 11 and 12 survive its end.

Annex 1: Details of processing

Item	Details
Subject matter	Provision of the Maestro platform and support under the MSA
Duration	The term of the MSA, plus up to 90 days for return and deletion
Nature and purpose	Hosting, storing, retrieving and analysing content; generating AI outputs; running workflows and integrations the Customer configures; voice and video calls with the Maestro assistant; support and security monitoring
Categories of data subjects	The Customer's staff and authorised users; people whose data appears in content the Customer uploads or connects (for example clients, counterparties, suppliers); people the assistant speaks with on calls the Customer sets up [●]
Types of personal data	Identity and contact details; account and usage data; content of prompts, documents, messages, emails and calendar items the Customer connects; call audio and video processed live; AI outputs [●]
Special category data	Not intended. The Customer will not upload special category or criminal-offence data unless agreed in the order form with any extra safeguards [●]
Live audio and video	Processed in memory during a call and not stored after it ends, unless the Customer turns on recording. Signals about tone are used only to adapt the assistant's speech in that call, are not stored and are not used to profile anyone
Emotion signals and staff	Where the users of a feature are the Customer's own staff in the EU, tone reading is switched off
Hosting region	[EU (Stockholm)] / [other region agreed in the order form]
Retention	Content kept for the term, or shorter on the Customer's instruction; deleted within 90 days after the end; security logs kept for [●]

Annex 2: Technical and organisational measures

Area	Measures
Access control	Two-factor sign-in, which the Customer's admins can make mandatory; role-based permissions, teams and an access inspector; least-privilege access for Promethean staff; access removed promptly when no longer needed
Separation of customers	Each customer has its own application instance and database [confirm]; application-level workspace scoping plus database row-level security on tenant tables
AI actions	Every AI tool call is classified by risk, reversibility and data sensitivity and passes a policy gate; actions needing approval wait for a person; each executed action produces an audit record
Encryption	TLS 1.3 in transit; database encrypted at rest; object storage encrypted at rest [confirm]
Infrastructure	Hosted on AWS in the agreed region; no public route to the database; administrative access through a bastion without inbound SSH; secrets held in AWS Secrets Manager and read at runtime; infrastructure defined as code (Terraform)
AI processing	Model, speech-to-text, video and document search run on infrastructure Promethean controls; no customer content sent to third-party AI model providers
Logging and monitoring	Application and security logs with restricted access; audit log of user and AI actions available to the Customer's admins
Availability and backup	Database replicated across two availability zones; automated daily backups kept for 7 days; deletion protection on
Incident management	Documented incident response with notification under clause 8; root-cause and remediation report
People	Confidentiality obligations for all staff and contractors; security awareness for anyone with access to customer data
Testing	Independent penetration test [before go-live / yearly] [●]
Development	Code reviewed before release [confirm]; changes deployed through a controlled pipeline with feature flags

Annex 3: Subprocessors

Subprocessor	Service	Data	Location
Amazon Web Services EMEA SARL	Hosting: application, database, files, logs, backups	All Customer Personal Data at rest	EU (Stockholm) unless agreed otherwise
Vast.ai	GPU servers for the model, voice and avatar	Content in use during processing	Varies by server; may be outside the UK and EEA [restrict to EU servers]
Pipedream, Inc.	Integrations the Customer switches on	Data passed to the connected application	United States
Stripe Payments Europe, Ltd.	Billing and payment	Billing contact and payment details	EU and United States
Unstructured	Parsing uploaded documents	Document content	United States

Contracting entity names to be checked against each provider's current terms. Pipedream is used only if the Customer turns on an integration. Promethean will update this list under clause 6.

Annex 4: Transfer mechanisms

- Transfers from the EEA to a country without an adequacy decision: the EU Standard Contractual Clauses (Commission Decision 2021/914), Module 3 (processor to processor), with a transfer risk assessment.
- Transfers from the UK: the UK International Data Transfer Agreement, or the UK Addendum to the EU Standard Contractual Clauses.
- Transfers to the United States: the EU–US Data Privacy Framework and its UK extension where the recipient is certified; otherwise the clauses above.
- Transfers between the UK and the EEA rely on the adequacy decisions in each direction.

Signed for the Customer: _____ Name, title, date

Signed for Promethean Systems Ltd: _____ Federico Nordenstahl, Director, date