Data Processing Agreement (DPA)

Version 2.0 | Revised: August 2026 | Supersedes the version revised June 2025

Scope and Applicability

1.1 This Data Processing Agreement (the "DPA") applies to any processing of personal data carried out under the Master Services Agreement (the "MSA") between the parties.

1.2 The processing of personal data shall be governed by the applicable data protection laws of the country where the Data Controller is established, and by the terms of the MSA and this DPA.

1.3 In the event of a conflict between the MSA and this DPA, the provisions of this DPA shall prevail, but only with respect to the conflicting subject matter and only to the extent required by Applicable Data Protection Law. The limitations and exclusions of liability set out in the MSA continue to apply to this DPA in accordance with Section 14.2.

1.4 Terms not defined in this DPA shall have the meaning assigned to them in the MSA.

1.5 This DPA applies to the processing activities described in Section 3, which identifies, for each activity, whether Prometeo acts as a Data Processor or as a Data Controller.

2. Definitions

For the purposes of this DPA, the following terms shall have the meanings set out below:

Applicable Data Protection Law	The data protection and privacy laws of the country where the Data Controller is established, together with any other data protection law applicable to the processing carried out under this DPA.
Personal Data	Any information relating to an identified or identifiable natural person. In some jurisdictions, this may also include data relating to legal entities.
Data Controller ("Controller")	The natural or legal person who determines the purposes and means of processing personal data.
Data Processor ("Processor")	The natural or legal person who processes personal data on behalf of the Controller, in accordance with the Controller's instructions.
Sub-processor	Any third party engaged by the Processor to perform specific processing activities on behalf of and under the instructions of the Controller.
Processing	Any operation performed on personal data, whether automated or not, including collection, recording, organization, structuring, storage, adaptation, use, disclosure, deletion, or destruction.
Data Subject	The individual to whom the personal data relates.
Data Breach (also: Security Incident or Incident)	Any event that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.
Aware	Prometeo is "Aware" of a Data Breach when its security function has confirmed, with a reasonable degree of certainty, that a Data Breach affecting personal data processed under this DPA has occurred. Alerts, anomalies and events still under investigation that have not been so confirmed do not, by themselves, constitute awareness.
International Data Transfer	The transmission of personal data to a country other than the one in which it was originally collected, whether to another Controller or Processor, for the purpose of processing.
Standard Contractual Clauses ("SCCs")	The standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission under Implementing Decision (EU) 2021/914, as incorporated in Annex II.

3. Roles of the Parties

3.1 Prometeo acts as Data Processor on behalf of the Client with respect to the personal data that the Client provides, or makes accessible to Prometeo, for the delivery of the contracted services. This includes the Account Validation solution and the retrieval of banking data through the Prometeo API.

3.2 Prometeo acts as Data Controller with respect to the following limited activities only, which it carries out for its own purposes and under its own legal basis:

(a) security, audit and access logs generated by the Prometeo platform, processed for information security, fraud and abuse prevention, and compliance with legal obligations binding on Prometeo;

(b) system telemetry and performance metrics, processed for service availability, capacity management and troubleshooting;

(c) the contact details of the Client's personnel, processed for contract administration, billing and service communications.

3.3 The activities listed in Section 3.2 do not extend to the content of end user banking data. Where personal data processed under Section 3.2 is not required for the stated purpose, it is masked, pseudonymized or excluded before processing.

3.4 Prometeo shall not act as Data Controller with respect to any processing activity other than those listed in Section 3.2 without the Client's prior written agreement.

3.5 Each party remains responsible for compliance with Applicable Data Protection Law in respect of the activities for which it acts as Data Controller.

4. Principles

Both parties agree to process personal data in accordance with the following principles. These principles form binding obligations and are intended to promote a consistent and high standard of data protection across all activities governed by this DPA:

Lawfulness, fairness and transparency	Personal data must be processed lawfully, fairly and in a transparent manner. A valid legal basis must support each processing activity (for example, consent, contract, legal obligation or legitimate interest). Data Subjects must be clearly informed about how their data is collected, used and protected.
Purpose limitation	Personal data shall be collected for specific, explicit and legitimate purposes, and must not be further processed in a way that is incompatible with those purposes. The Processor must process data strictly in accordance with the Controller's instructions.
Data minimization	Only the personal data that is strictly necessary to achieve the stated purpose may be processed. Unnecessary or excessive data must not be collected or retained.

Accuracy	Personal data must be accurate and, where necessary, kept up to date. Inaccurate or outdated data must be corrected or deleted without delay.
Storage limitation	Data must be retained only for as long as necessary to fulfil the intended purpose or to comply with legal obligations. After that, it must be securely deleted or anonymized.
Integrity, confidentiality and security	Personal data shall be processed in a way that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures.
Accountability	The Controller is responsible for ensuring compliance with these principles and must be able to demonstrate such compliance. The Processor shall support the Controller by implementing appropriate measures, such as privacy by design and by default, data protection impact assessments where required, and the appointment of a Data Protection Officer where legally necessary.

5. Purpose of the Data Processing Assignment

5.1 Prometeo, acting as Data Processor in accordance with Section 3.1, provides the Client with various technological solutions as part of the contracted services. The use of these services necessarily involves the processing of personal data, as defined under Applicable Data Protection Law.

5.2 The personal data is provided by the Client, acting as Data Controller, who authorizes Prometeo to process it on their behalf, solely for the purpose of delivering the contracted services and in accordance with the Client's instructions.

6. Identification of the Personal Data Involved

To properly deliver the contracted services, the Client shall provide Prometeo with the personal data necessary for their execution. This may include, by way of example:

- Full name
- Email address
- Tax identification number
- Phone number
- Bank account number
- Any other data required to fulfil the scope of the service

7. Obligations of Prometeo as Data Processor

Prometeo, acting as Data Processor, undertakes to:

7.1 Legal compliance

Comply with all obligations applicable to data processors under Applicable Data Protection Law and any other binding legal provisions.

7.2 Purpose limitation and restrictions on use

Process personal data solely for the purposes set out in this DPA and the Controller's documented instructions. Prometeo shall not use the personal data for its own purposes. Without limiting the foregoing, Prometeo shall not:

(a) sell, rent, lease or otherwise make personal data available to any third party other than a Sub-processor authorized under Section 9;

(b) use personal data for advertising, marketing or profiling purposes;

(c) use personal data to train, fine tune, validate or otherwise develop machine learning or artificial intelligence models, whether for Prometeo's own benefit or that of a third party;

(d) combine personal data with data obtained from other clients or sources, except as strictly necessary to deliver the contracted services and as instructed by the Controller.

Pending internal confirmation before signature

If Prometeo uses aggregated data derived from the services to maintain or improve banking connectivity, the following sentence must be added to Section 7.2 and the position must be reflected in the compliance questionnaire: "Prometeo may use aggregated data derived from the services solely to maintain, secure and improve banking connectivity, provided that such data is irreversibly anonymized so that no Data Subject can be identified, directly or indirectly, and is not attributable to the Client. Anonymized data is not personal data and its use is not subject to the restriction in Section 7.2(c)."

If Prometeo does not use such data, this box is deleted and Section 7.2 stands as drafted.

7.3 Transparency, cooperation and audit

Provide the Controller with all necessary information to demonstrate compliance with this DPA. Prometeo shall respond to reasonable audit and assurance requests within ten (10) business days of a written request, by providing its current ISO/IEC 27001 certificate, the executive summary of its most recent independent penetration test, and the security and privacy policies relevant to the services. On site audits may be conducted once per contract year, with thirty (30) calendar days' prior written notice, subject to confidentiality and to reasonable restrictions necessary to protect the security and continuity of the services and the data of other clients.

7.4 Authorized personnel

Ensure that any personnel authorized to process personal data:

- are bound by a written confidentiality obligation;

- have received appropriate data protection training; and
- process data only in accordance with the Controller's instructions or applicable legal requirements.

7.5 Security measures

Implement and maintain appropriate technical, physical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized access or disclosure. These measures shall include, at a minimum:

- pseudonymization and encryption, in transit and at rest, where appropriate;
- measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore access to personal data in a timely manner in the event of an incident;
- role based access control and multi factor authentication for access to production environments;
- masking or redaction of full account numbers, credentials and secrets in logs, support tickets and monitoring dashboards;
- regular testing and evaluation of the effectiveness of the implemented security measures.

7.6 Recordkeeping and supervision

Maintain records of processing activities as required by law and make them available to the Controller or the competent authority upon request. Cooperate fully with any regulatory audit or investigation.

8. Data Subject Rights

8.1 Prometeo shall implement appropriate technical and organizational measures, considering the nature of the processing, to assist the Controller in responding to requests from Data Subjects exercising their rights under Applicable Data Protection Law.

8.2 If Prometeo receives a Data Subject request directly, it shall notify the Controller within five (5) business days and provide all relevant information necessary for the Controller to respond appropriately.

8.3 If the data is processed exclusively through systems managed by Prometeo, and if agreed with the Controller, Prometeo may respond directly to the request on the Controller's behalf, in accordance with applicable legal deadlines. The Controller must still be informed of the request and of the response provided.

9. Sub-processing

9.1 The Client provides a general written authorization for Prometeo to engage Sub-processors for the performance of the services. The Sub-processors engaged as at the date of this DPA are listed in Annex I.

9.2 Prometeo shall keep Annex I up to date and shall make the current list available to the Client on request.

9.3 Prometeo shall give the Client at least thirty (30) calendar days' prior written notice before engaging a new Sub-processor or replacing an existing one. The notice shall identify the Sub-processor, the processing activity it will perform, the categories of personal data concerned, and the countries in which it will process that data.

9.4 The Client may object to a new or replacement Sub-processor on reasonable data protection grounds within fifteen (15) calendar days of the notice. The parties shall discuss the objection in good faith. If the objection is not resolved within thirty (30) calendar days, the Client may terminate the affected services on written notice, without penalty and without early termination charges, and Prometeo shall refund any fees prepaid in respect of the period after termination.

9.5 Where a Sub-processor must be replaced urgently to preserve the security or continuity of the services, Prometeo may make the replacement before the notice period in Section 9.3 has elapsed, provided that it notifies the Client without undue delay and in any event within five (5) business days. The objection right in Section 9.4 applies from the date of that notice.

9.6 Prometeo shall impose on each Sub-processor, by written contract, data protection obligations that are no less protective than those set out in this DPA, including appropriate technical and organizational measures and breach notification obligations.

9.7 Prometeo remains fully liable to the Client for the acts and omissions of its Sub-processors as if they were its own.

10. International Data Transfers

10.1 The Client acknowledges that the services involve the processing and storage of personal data in the United States, in the cloud region identified in Annex I.

10.2 Prometeo shall not transfer personal data to a country other than the country in which it was collected unless a transfer mechanism recognized under Applicable Data Protection Law is in place. Depending on the law applicable under Section 1.2, that mechanism may be: an adequacy decision or an equivalent recognition of an adequate level of protection; the Standard Contractual Clauses set out in Annex II; binding corporate rules; another mechanism expressly permitted by Applicable Data Protection Law; or, where permitted, the informed consent of the Data Subject obtained by the Controller.

10.3 Where the Data Controller is established in the European Economic Area, in the United Kingdom or in Switzerland, the Standard Contractual Clauses set out in Annex II are incorporated into this DPA by reference and apply to transfers of personal data from the Controller to Prometeo. Module Two (controller to processor) applies. In the event of a conflict between those clauses and the remainder of this DPA, the Standard Contractual Clauses prevail in respect of the transfer.

10.4 Prometeo shall notify the Client at least thirty (30) calendar days before changing the country or cloud region in which personal data is stored. The objection and termination rights set out in Section 9.4 apply to that change.

10.5 Prometeo shall provide the Client with the information reasonably necessary for the Client to carry out a transfer impact assessment, including information on the legal regime applicable to Prometeo and its Sub-processors in the destination country.

10.6 If Prometeo receives a legally binding request from a public authority for access to personal data processed under this DPA, Prometeo shall: notify the Client without undue delay, unless legally prohibited from doing so; where prohibited, use reasonable efforts to obtain a waiver of that prohibition; challenge requests that appear unlawful or excessive; and disclose only the minimum amount of data reasonably required.

11. Security Breach Notification

11.1 Prometeo shall notify the Controller of a Data Breach affecting personal data processed under this DPA without undue delay, and in any event within twenty four (24) hours of becoming Aware of it, as that term is defined in Section 2.

11.2 The initial notification may contain partial information where a complete assessment is not yet available. Prometeo shall provide supplementary information as it becomes available, and in any event sufficiently in advance of any notification deadline applicable to the Controller under Applicable Data Protection Law.

11.3 The notification shall include, to the extent known at the time:

- a description of the incident and how it was detected;
- the categories and estimated number of affected Data Subjects and records;
- the likely consequences of the breach;

- the measures taken or planned to address and mitigate the breach;
- contact details for further information or coordination.

11.4 Prometeo shall preserve the forensic evidence relating to the incident and shall deliver a written root cause analysis within five (5) business days of containment, covering the timeline, the root cause, the affected components, the corrective actions taken and the preventive measures adopted.

11.5 Where legally required, Prometeo shall cooperate with the Controller in notifying the competent supervisory authority and the affected Data Subjects.

11.6 A notification made under this Section is not, in itself, an acknowledgement of fault or liability by Prometeo.

12. Obligations of the Client as Data Controller

The Client, acting as Data Controller, shall be solely responsible for the following obligations:

12.1 Lawful basis for processing

Ensure that all personal data provided to Prometeo is processed on a valid legal basis, in accordance with Applicable Data Protection Law. The Client must be able to demonstrate this basis upon request.

12.2 Instructions to the Processor

Provide Prometeo with clear, lawful and written instructions regarding the processing of personal data. Instructions must include the purpose and scope of processing, the duration of the processing, the nature and categories of personal data, the categories of Data Subjects, and the specific obligations and rights of the Client that Prometeo must support.

12.3 Transparency and information duties

Inform Data Subjects, in a clear and lawful manner, about the processing of their personal data, in compliance with applicable transparency requirements. This includes obtaining and recording the consent or authorization required before Prometeo is instructed to access an end user bank account.

12.4 Data Subject rights

Implement procedures and channels to allow Data Subjects to exercise their rights. Inform Prometeo of any request that involves data it processes, and provide the necessary instructions for response.

12.5 Monitoring and supervision

Actively monitor Prometeo's compliance with this DPA and Applicable Data Protection Law. This includes the right to conduct audits or assign an independent auditor, with reasonable notice and in accordance with Section 7.3.

12.6 Notification of personal data breaches

In the event of a Data Breach, the Client is responsible for assessing whether notification to the competent authority and to Data Subjects is required and, if so, for making that notification. Prometeo shall support this process as necessary.

12.7 Impact assessments and DPO

Where legally required, the Client shall conduct data protection impact assessments and appoint a Data Protection Officer.

13. Term, Return and Deletion of Personal Data

13.1 This DPA enters into force on the same date as the MSA and remains in effect for as long as Prometeo processes personal data on behalf of the Client.

13.2 Within thirty (30) calendar days of the termination or expiry of the services, Prometeo shall, at the Client's written choice: (a) return the personal data to the Client in a commonly used, machine readable format; or (b) delete the personal data and any copies of it.

13.3 If the Client does not communicate its choice within thirty (30) calendar days of termination, Prometeo shall delete the personal data.

13.4 Personal data contained in routine backups shall be deleted in accordance with Prometeo's standard backup cycle and in any event within ninety (90) calendar days of termination. Until deletion, that data remains subject to the security measures and confidentiality obligations of this DPA and is not processed for any other purpose.

13.5 Prometeo shall issue a written certificate of deletion within fifteen (15) business days of a written request from the Client.

13.6 Where retention is required by Applicable Data Protection Law or by another legal obligation binding on Prometeo, Prometeo shall store the data securely, block any further processing, and use the data solely to comply with that obligation. Prometeo shall inform the Client of the legal basis and of the expected retention period.

13.7 The confidentiality obligations set out in this DPA survive the termination of the services.

14. Liability, Governing Law and Jurisdiction

14.1 Liability. Each party shall be liable for any fines, damages or losses resulting from a breach of its own obligations under Applicable Data Protection Law and under this DPA.

14.2 Limitation of liability. Except where Applicable Data Protection Law provides otherwise, each party's liability under this DPA is subject to the limitations and exclusions of liability set out in the MSA. The parties agree that those limitations apply to the aggregate liability of each party under the MSA and this DPA taken together.

14.3 Indemnification. Each party agrees to indemnify and hold the other harmless from any claims, penalties, losses or proceedings arising from its own failure to comply with applicable data protection obligations.

14.4 Controller responsibility. The Client expressly acknowledges that Prometeo shall not be held liable for breaches that fall under the Client's responsibility as Data Controller, whether such obligations are expressly stated in this DPA or derive from Applicable Data Protection Law.

14.5 Governing law. This DPA shall be governed by the laws of the country in which the Data Controller is established.

14.6 Jurisdiction. Any disputes arising from or related to the processing of personal data under this DPA shall be submitted to the exclusive jurisdiction of the courts of the country where the Data Controller is located.

Annex I. Authorized Sub-processors

This Annex lists the Sub-processors authorized under Section 9.1 as at the date of this DPA. Prometeo shall keep this list current and shall notify the Client of any addition or replacement in accordance with Section 9.3.

Sub-processor	Service provided	Data accessed	Location
Amazon Web Services, Inc.	Cloud hosting, database storage and managed security infrastructure	Hosting and encrypted storage of personal data processed under the services. AWS personnel cannot access unencrypted customer data.	United States (region us-east-1)
Datadog, Inc.	Application performance monitoring and system telemetry logging	System metadata and masked application logs only. Account numbers and sensitive fields are masked prior to ingestion.	United States

Prometeo confirms that each Sub-processor listed above is bound by a written contract containing data protection obligations no less protective than those set out in this DPA, and that each holds current ISO/IEC 27001 or SOC 2 Type II assurance.

Annex II. Standard Contractual Clauses

II.1 Where Section 10.3 applies, the Standard Contractual Clauses adopted by the European Commission under Implementing Decision (EU) 2021/914 are incorporated into this DPA and executed by the parties. Module Two (transfer controller to processor) applies. The full text of the Standard Contractual Clauses shall be attached to and signed together with this DPA.

II.2 The optional docking clause in Clause 7 applies. The option in Clause 9(a) that applies is Option 2, general written authorization, with the notice period set out in Section 9.3 of this DPA. In Clause 11(a), the optional independent dispute resolution mechanism does not apply.

II.3 For the purposes of Clause 17, the Standard Contractual Clauses shall be governed by the law of the European Economic Area member state in which the Data Controller is established. For the purposes of Clause 18(b), disputes shall be resolved before the courts of that member state.

II.4 The annexes to the Standard Contractual Clauses are completed as follows:

- Annex I.A (List of parties): the data exporter is the Client, acting as Data Controller. The data importer is Prometeo, acting as Data Processor. The contact details are those set out in the MSA.
- Annex I.B (Description of the transfer): the categories of Data Subjects, categories of personal data, frequency, nature and purpose of the transfer, and retention period are those described in Sections 3, 6 and 13 of this DPA.
- Annex I.C (Competent supervisory authority): the supervisory authority of the European Economic Area member state in which the Data Controller is established.
- Annex II (Technical and organizational measures): the measures set out in Section 7.5 of this DPA.
- Annex III (List of Sub-processors): the Sub-processors listed in Annex I of this DPA.

Note for the Corporate Support review

This Annex incorporates the Standard Contractual Clauses by reference and completes their annexes. The full text of Implementing Decision (EU) 2021/914 must be attached before the DPA is signed with a Data Controller established in the European Economic Area, in the United Kingdom (with the UK International Data Transfer Addendum) or in Switzerland. For Data Controllers established in Latin America, Section 10.2 governs and this Annex does not apply.