Veros DPA Standard Template

This Data Processing Agreement (“DPA”) forms part of the Master Service Agreement between:

Veros Solutions B.V., a company incorporated under the laws of The Netherlands, with its registered office in ’s-Hertogenbosch (“Processor” or “Veros”)

and

[Customer Name] (“Controller” or “Customer”)

(together, the “Parties”).

This DPA applies where Veros processes Personal Data on behalf of the Controller in connection with the applicable Agreement and Terms of Service (“Agreement”).

This DPA forms part of and is governed by the Agreement.

1. Definitions

Capitalized terms not defined in this DPA have the meaning given to them in the Agreement or in Regulation (EU) 2016/679 (“GDPR”).

For the purposes of this DPA:

- “Agreement” means the Master Service Agreement entered into with Veros
- “Personal Data” means any personal data processed by Veros on behalf of Controller.
- “Data Protection Laws” means the GDPR and any applicable national data protection legislation.
- “Subprocessor” means any third party engaged by Veros to process Personal Data on behalf of the Controller.
- “Standard Contractual Clauses” or “SCCs” means the European Commission’s approved standard contractual clauses for international transfers of personal data.

2. Roles of the Parties

2.1 The Controller (Customer) acts as Data Controller.

2.2 Veros acts as Data Processor and processes Personal Data solely on behalf of the Controller and in accordance with documented instructions as set out in:

- The Agreement
- This DPA
- Any written instructions provided by the Controller

2.3 The Controller is responsible for ensuring that:

- It has a valid legal basis for processing Personal Data.
- It provides appropriate privacy notices to Data Subjects.
- Its instructions comply with Data Protection Laws.

3. Nature and Purpose of Processing

Veros processes Personal Data to provide the Veros Services, including:

- Hosting and storage of Customer Data
- Structuring, analyzing, and generating reports
- Facilitating collaboration workflows
- Providing AI-assisted functionality where enabled and configured by Customer

Categories of Data Subjects may include:

- Customer employees and contractors
- Representatives of suppliers, customers, brokers, or business partners
- Other individuals whose business contact details may be included in Customer Data

Categories of Personal Data may include:

- Names
- Business contact details
- User account information (email address, user ID, optional avatar)
- Technical identifiers (e.g., IP address, security metadata)
- Transaction-related identifiers that may relate to individuals (where included by Customer)

Processing is limited to what is necessary to provide the Services.

4. Processor Obligations

Veros shall:

4.1 Process Personal Data only on documented instructions from the Controller.

4.2 Ensure that persons authorized to process Personal Data:

- Are bound by confidentiality obligations.
- Receive appropriate security awareness training.

4.3 Implement appropriate technical and organizational measures in accordance with Article 32 GDPR.

These measures are described in Veros' Security Policy and include, among others:

- Data Hosting within the EU
- AES-256 encryption at rest
- TLS 1.2+ encryption in transit
- Role-based access control
- Logical tenant separation
- Audit logging of user activity
- Encrypted backups with point-in-time recovery

4.4 Assist the Controller in responding to:

- Data Subject access requests
- Requests for rectification, erasure, restriction, or portability

4.5 Notify the Controller without undue delay after becoming aware of a Personal Data Breach affecting Controller data, and provide sufficient information to support regulatory reporting obligations.

5. Subprocessors

5.1 Use of Subprocessors

The Controller acknowledges and agrees that Veros uses Subprocessors in the normal course of providing the Services.

5.2 Current Subprocessors

Veros maintains a current list of Subprocessors internally, which is made available upon request.

5.3 Changes to Subprocessors

Veros may update or replace Subprocessors from time to time.

In the event a new Subprocessor is engaged that processes Personal Data, Veros will:

- Inform the Controller in advance where reasonably possible.
- Ensure that appropriate data protection obligations are imposed on the Subprocessor.

5.4 Subprocessor Safeguards

Veros ensures that all Subprocessors:

- Are subject to written agreements containing data protection obligations.
- Provide appropriate safeguards under Data Protection Laws.

Veros remains responsible for the performance of its Subprocessors.

6. International Data Transfers

All customer data is stored and processed within the European Union.

Certain optional features or enterprise configurations may involve transfers outside the EU/EEA.

Where such transfers occur, Veros ensures appropriate safeguards, including:

- Reliance on European Commission adequacy decisions; or
- Execution of Standard Contractual Clauses (SCCs); and
- Supplementary technical measures such as encryption in transit and at rest.

The Controller acknowledges that use of such optional features may result in international data transfers covered by SCCs.

7. Data Subject Rights

Veros shall:

- Promptly notify the Controller if it receives a Data Subject request relating to Personal Data.
- Not respond directly to such requests unless legally required or instructed by the Controller.

Taking into account the nature of processing, Veros shall provide reasonable assistance to enable the Controller to fulfill its obligations under Articles 15–22 GDPR.

8. Data Protection Impact Assessments

Upon reasonable request, Veros shall provide information necessary to support:

- Data Protection Impact Assessments (Article 35 GDPR)
- Prior consultations with Supervisory Authorities (Article 36 GDPR)

Such assistance is limited to information available to Veros in its role as Processor.

9. Deletion and Return of Data

Upon termination of the Agreement, Customer data is deleted within 30 days, unless otherwise agreed.

Backup systems follow standard retention cycles.

10. Audit Rights

Audits shall be conducted primarily through documentation review, certifications, and remote assessments.

On-site audits shall only be permitted where strictly required by applicable law and subject to prior written agreement, reasonable notice, and appropriate confidentiality safeguards.

Audits must not compromise the security, integrity, or confidentiality of other customers or the Veros infrastructure.

11. Confidentiality

Confidentiality obligations are governed by the Agreement.

12. Governing Law and Jurisdiction

This DPA forms part of and is governed by the Agreement. The governing law and jurisdiction provisions of the Agreement apply to this DPA.

13. Order of Precedence

In the event of any conflict between the terms of this DPA and the Agreement (including the Terms of Service), the terms of this DPA shall prevail solely with respect to matters relating to the processing of Personal Data and compliance with applicable Data Protection Laws.

For all other matters, the terms of the Agreement shall prevail.