Data Processing Agreement

Shipping Technology B.V.

Veerkade 7D, 3016 DE Rotterdam

Explanation

This agreement aims to establish a clear framework for the collaboration between the Client and the Contractor with regard to the **Processing of Personal Data**.

This **Data Processing Agreement ("Processing Agreement")** applies to all processing of personal data by **Shipping Technology B.V.**, located in Rotterdam ("Processor"), on behalf of its customers ("Controller").

This document has been prepared by Shipping Technology B.V.

Appendix 1 explicitly specifies which particular data are applicable in the cooperation between both parties and to which this agreement applies.

Shipping Technology and the other party agreeing to these conditions ("Customer") have entered into an agreement for the provision of the Services for processors (as amended from time to time, the "Agreement").

If you accept these Data Processing Terms on behalf of a Customer, you guarantee the following:
(a) you have full legal authority to bind the Customer to these Data Processing Terms,
(b) you have read and understood these Data Processing Terms, and
(c) you agree to these Data Processing Terms on behalf of the Customer.

If you do not have the legal authority to bind the Customer, you must not agree to these Data Processing Terms.

The undersigned:

Shipping Technology B.V. ("Shipping Technology", "we", "us", "our"), located at **[Veerkade 7D, 3016 DE Rotterdam]**, is responsible for the processing of personal data as described in this privacy statement. Hereinafter referred to as the **"Processor"**.

And its customers, hereinafter referred to as the **"Controller"**.

Whereas:

The Controller wishes to make use of the services of the Processor for the purpose of carrying out the assignment agreed between the Processor and the Controller.

The Parties record their mutual rights and obligations in this Agreement.

The Parties declare that they have agreed as follows:

Article 1 — Definitions

The definitions used in this Agreement correspond to the definitions used in **Article 4 of the GDPR**:

Processor:
A natural or legal person who processes personal data on behalf of the Controller.

Controller:
A natural or legal person who determines the purposes and means of the processing of personal data.

Sub-processor:
Another processor engaged by the Processor to carry out specific processing activities on behalf of the Controller.

Data Subject:
The person to whom the Personal Data relates.

Personal Data:
Any information relating to an identified or identifiable natural person (the data subject).

Processing:
An operation or set of operations performed on personal data or sets of personal data, whether or not by automated means.

Data Breach:
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

The Parties ensure compliance with applicable laws and regulations concerning the processing of Personal Data, as well as the agreements set out in this Agreement.

Article 2 — Applicability and Duration

This Agreement enters into force upon signature by the Parties on the date of the contract with the Customer with regard to the processing activities carried out by the Processor on behalf of the Controller.

This Agreement ends when no Personal Data are processed within the scope of this Agreement. Articles which by their nature should remain applicable after termination — including but not limited to **Article 9 (Confidentiality)** and **Article 10 (Provision & deletion)** — shall remain fully in force after termination.

This Agreement cannot be terminated prematurely.

The Parties — partly in execution of Article 28(3) GDPR — wish to record several conditions in this supplementary agreement ("Processing Agreement") applicable to their relationship concerning the activities carried out on behalf of the Controller.

Article 3 — Subject of the Processing Agreement

The Controller is responsible for the processing of Personal Data in the execution of this Agreement. The Processor has no independent authority over the Personal Data.

The personal data processed by the Processor within the framework of this Processing Agreement as referred to in paragraph 1 are listed in **Appendix 1**.

The Processor processes Personal Data only on behalf of the Controller within the framework of executing this Agreement, in accordance with the purposes, means, and retention periods determined by the Controller and described in Appendix 1, as well as any other written instructions provided by the Controller, unless Union or Member State law requires the Processor to process the data. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such notification for important public interest reasons.

The Controller guarantees that its instructions to the Processor lead to processing that complies with applicable laws and regulations and does not infringe the rights of third parties.

Article 4 — Technical and Organizational Measures (Security)

The Controller shall only provide Personal Data to the Processor if it has ensured that appropriate security measures have been implemented, guaranteeing an adequate level of protection in accordance with Article 32 GDPR.

The Controller is entitled to verify, in consultation, the measures and compliance with the obligations resting on the Processor. The costs of such verification shall be borne by the Controller.

Article 5 — Data Breaches & Notification Obligation

If the Processor becomes aware of a **security breach (data breach)** as defined in Article 1 of this Agreement, the Processor shall inform the Controller as soon as possible, but no later than **72 hours after becoming aware of the breach**.

The notification shall at least include:

- the nature of the incident or breach
- the (possible) affected Personal Data
- the known or expected consequences of the breach
- the proposed solution
- measures already taken by the Processor

The Controller is responsible, where necessary, for reporting data breaches to the **Dutch Data Protection Authority** and possibly to the affected data subjects.

The Controller is responsible for maintaining the **Data Breach register**.

If, despite the Processor implementing agreed measures, a Data Breach occurs, the Controller cannot hold the Processor liable for damages suffered as a result.

Article 6 — Engagement of Third Parties

The Processor will not outsource obligations arising from the Agreement to third parties unless prior consent from the Controller has been obtained.

OR

The Controller grants the Processor permission to use a **sub-processor** when processing personal data under this Processing Agreement, provided that:

- the Controller may object
- the sub-processor signs a **Sub-processing Agreement** with equivalent or stricter obligations
- the Processor supervises compliance by the sub-processor
- a copy of the agreement can be provided upon request

If the data are processed outside the **EEA**, the Controller receives a signed **EU Standard Contractual Clauses** document (Appendix 3).

The Processor remains responsible for the actions or omissions of the sub-processors.

Article 7 — Transfer to Third Countries

The Processor is not permitted to transfer Personal Data to countries outside the European Union unless:

- the Controller has explicitly given written consent, and
- such transfer is permitted under applicable European privacy legislation.

Where data are transferred to a sub-processor in a country without an adequate protection level, the transfer shall be governed by **European Commission Standard Contractual Clauses**, attached as Appendix 3.

Article 8 — Assistance & Requests from Data Subjects

If a Data Subject submits a request to the Processor regarding access, correction, modification, or restriction, the Processor will immediately forward the request to the Controller and inform the Data Subject accordingly.

The Controller will respond to such requests **without undue delay and within 14 days**.

The Processor assists the Controller, where possible, with appropriate technical and organizational measures to comply with requests under **Chapter III GDPR** and requests from supervisory authorities.

The Processor may charge reasonable costs for such assistance after prior consultation.

Article 9 — Confidentiality

The Processor, its employees, and any sub-processors with access to Personal Data shall maintain confidentiality regarding Personal Data unless a legal obligation requires disclosure.

This obligation does not apply where:

- the Controller has explicitly permitted disclosure, or
- disclosure is logically necessary for executing the Agreement.

The Processor ensures that employees and third parties engaged by it are contractually bound by the same confidentiality obligations.

The Processor immediately informs the Controller of any request to access or disclose Personal Data in violation of this confidentiality obligation.

Article 10 — Provision & Deletion

The Processor ensures that Personal Data and any copies are returned to the Controller or destroyed after completion of the agreed services, unless storage is legally required.

Upon request, the Processor will demonstrate compliance with this article.

Costs related to collecting and transferring Personal Data after termination shall be borne by the Controller.

Article 11 — Liability & Insurance

Both Parties ensure that processing under this Agreement does not violate the rights of Data Subjects.

Each Party is responsible for its own actions.

If the Processor is liable to the Controller for damages, liability is limited to **direct damages** resulting from attributable failure or unlawful acts.

Total liability shall never exceed an amount reasonably proportional to the costs of executing the assignment.

Liability limitations do not apply in cases of:

- intent or gross negligence
- loss of Personal Data
- fines imposed by supervisory authorities due to the Processor's fault.

The Processor is not liable for **indirect damages**, including loss of profit, financial loss, or immaterial damages.

Article 12 — Control & Supervision

The Controller may inspect compliance at its own expense provided that:

- five (5) working days' notice is given
- the inspection does not unreasonably disrupt the Processor's business operations.

Internal costs of the Processor remain at its own expense.

If during inspection it appears that the Processor does not comply with the Agreement, the Processor must take all necessary measures to ensure compliance.

Article 13 — Costs

Costs related to normal processing activities under the Agreement are deemed included in the fees agreed in the Agreement.

Article 14 — Amendment of the Agreement

Amendments to this Processing Agreement are only possible with written consent of both Parties.

If any provision becomes invalid or must be amended due to changes in privacy legislation, the remaining provisions remain valid.

Parties will replace invalid provisions with new provisions that best reflect the intent of the original provision.

If amendments require significant changes to the underlying assignment, or the Processor cannot ensure adequate protection, the Processor may terminate the Agreement.

Article 15 — Miscellaneous Provisions

In case of conflict between this Processing Agreement and other agreements between the Parties, this **Processing Agreement prevails**.

Dutch law applies to this Agreement.

Disputes shall be submitted exclusively to the competent court in the **district of Rotterdam**.

Signature

Processor (Shipping Technology)

Place: Rotterdam
Date: TO BE COMPLETED
Name: TO BE COMPLETED

Appendix 1

Explanation

This appendix defines the **full scope of personal data processed by Shipping Technology** as Processor during the execution of the assignment covered by this Processing Agreement.

This includes:

- purposes and means of processing
- types of data processed
- possible sharing with third parties

This appendix consists of a general section and a section specific to the assignment.

The Controller is responsible for informing data subjects (e.g., website visitors) about these processing activities.

Personal Data

- Name, email address, phone number
- IP address and technical device data
- Location data
- Cookie data and website/product usage data
- Information provided when creating an account or contact form
- Payment or billing data (if applicable)

Purposes of Processing

Newsletter / Marketing Communication

Collected data: email address
Legal basis: consent
Retention period: until unsubscribed.

Performance of a Contract

Collected data: name, email, phone number, billing data
Legal basis: execution of contract
Retention period: as long as necessary for service delivery and according to legal obligations.

Contact and Support

Collected data: email, phone number, message content
Legal basis: legitimate interest or contract execution.

Website Analysis and Improvement

Collected data: IP address, cookie data, browser data
Legal basis: consent for non-essential cookies.

Legal Obligations

Collected data: information required for fiscal or legal purposes.

Sub-processors

We do not sell Personal Data to third parties. Personal Data are only shared:

- with service providers processing data on our behalf
- if required by law or supervisory authority
- with third parties necessary to deliver the service.

We conclude **data processing agreements** with processors to ensure an equivalent level of protection.

ANNEX 2 – TECHNICAL AND ORGANISATIONAL MEASURES

The Processor shall implement appropriate technical and organisational measures to protect Personal Data against loss, unauthorised access, alteration, disclosure or other unlawful Processing. In determining these measures, the nature of the Processing, the risks, the state of the art and the costs of implementation shall be taken into account.

The following measures apply:

1. Access control

- Access to Personal Data is granted only to authorised persons who require such access to perform their duties.
- Users are provided with individual user accounts.
- Access rights are periodically reviewed and are adjusted or withdrawn following termination of employment or a change of role.
- Multi-factor authentication is used where possible for administrator accounts and remote access.

2. Confidentiality

- Personnel with access to Personal Data are subject to confidentiality obligations.
- Personnel are informed of their responsibilities regarding privacy and information security.
- Personal Data is not made available to unauthorised persons.

3. Security of systems and data

- Systems are appropriately protected through measures including password policies, firewalls, malware protection and security updates.
- Personal Data is encrypted during transmission through secure connections.
- Personal Data is encrypted or pseudonymised at rest where appropriate.
- Production environments are separated from testing and development environments.

4. Availability and recovery

- Relevant Personal Data and systems are backed up periodically.
- Backups are appropriately secured and access is restricted.
- The Processor maintains procedures for restoring Personal Data and systems following a disruption or incident.
- Backups and recovery procedures are periodically tested.

5. Logging and monitoring

- Relevant access to and activities within systems are logged where appropriate.
- Log data is protected against unauthorised access and alteration.
- Unusual or suspicious activities are investigated.

6. Security incidents and Personal Data Breaches

- The Processor maintains a procedure for reporting, investigating and handling security incidents.
- A potential Personal Data Breach shall be reported to the Controller without undue delay.
- The Processor shall assist the Controller in investigating and, where necessary, reporting a Personal Data Breach.

Incident contact: **security@shippingtechnology.com**

7. Retention and deletion

- Personal Data shall not be retained for longer than necessary to provide the agreed services.
- Following termination of the services, Personal Data shall be deleted or returned, unless further retention is required by law.
- Data carriers shall be securely erased or destroyed before disposal or reuse.

8. Review and improvement

- The Processor periodically assesses whether the security measures remain appropriate and effective.
- Identified deficiencies are remediated within an appropriate period.
- The measures are adjusted where changes in the services, technology or risks require this.

9. Additional information

- **Relevant certifications:** ISO27001
- **Date of last review:** 25-08-2026