Data Processing Agreement

DRAFT, pending legal review

Last updated: 11 June 2026

In short: This DPA applies when e-tailize processes personal data for a business customer as processor and the customer acts as controller. It is a draft Article 28 GDPR agreement and should be reviewed with the main Terms and order form.

Placeholders to confirm:

1. Parties and role

This DPA is between the Customer named in the signed order form as controller and e-tailize B.V. as processor, unless the order form states a different role allocation. It forms part of the Terms and any signed order form between the parties.

2. Subject matter and duration

The subject matter is the processing of personal data needed to provide the Marketplace Scan, marketplace onboarding, Platform, integrations, AI chat and support. Processing continues for the term of the Services and any permitted retention period after termination.

3. Nature and purpose of processing

- Hosting, storing and transmitting Customer Data.
- Processing catalogue, order, account and support data.
- Synchronising data with connected marketplaces and integrations.
- Operating AI-assisted workflows requested by the Customer.
- Providing support, security monitoring and troubleshooting.

4. Types of data and data subjects

The Services are not intended for special categories of personal data. The Customer must not submit such data unless it is strictly necessary and lawful, and remains responsible for the lawfulness of any special category data it provides.

Names, emails, roles, account identifiers, support communications and IP addresses | Customer staff and authorised users

Order data, delivery details and marketplace account data where provided by the Customer | Customer buyers, marketplace users and business contacts

Developer identifiers, API usage data and integration logs | Developers and technical users

5. Customer instructions

e-tailize processes personal data only on documented Customer instructions, including the Terms, order form, this DPA and Customer configuration in the Services.

If e-tailize believes an instruction infringes GDPR or EU member state data protection law, it will inform the Customer unless prohibited by law.

6. Confidentiality
e-tailize ensures that persons authorised to process personal data are bound by confidentiality obligations.

7. Security measures
e-tailize implements appropriate technical and organisational measures considering the nature, scope, context and risk of processing.
These include encryption in transit and at rest, role based access control with least privilege, multi factor authentication for staff access, backups, logging and monitoring, vendor security assessment, and staff confidentiality obligations.

8. Sub-processors
The Customer gives general authorisation for e-tailize to use sub-processors needed to provide the Services.
The current sub-processors, their countries and purposes, are listed in the Privacy Policy under Recipients and sub-processors.
e-tailize will give notice of material sub-processor changes and provide a reasonable objection mechanism where required by GDPR.

9. Data subject rights and compliance assistance
e-tailize will reasonably assist the Customer with data subject requests, security obligations, DPIAs and regulator consultation where required under GDPR and where the Customer cannot reasonably handle the request without e-tailize help.
e-tailize may charge reasonable costs for assistance that goes beyond what GDPR requires from a processor.

10. Personal data breach
e-tailize will notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer personal data.
The operational breach contact is support@e-tailize.com. The notification will include available information needed by the Customer to assess notification duties.

11. End of processing
At the end of the Services, e-tailize will delete or return personal data according to Customer instructions, unless retention is required by EU or member state law.
Retention and deletion follow the retention periods in the Privacy Policy, unless the order form states otherwise.

12. Audit

e-tailize will make information reasonably necessary to demonstrate compliance available to the Customer. Audits take place at most once per calendar year, with 30 days written notice, during business hours, under confidentiality and at the Customer’s cost. e-tailize first provides existing audit reports and documentation; an on site audit only takes place where those are reasonably insufficient.

13. Liability

Liability under this DPA is subject to the limitations and exclusions in the Terms, unless GDPR or mandatory law requires otherwise.

Each party bears regulatory fines imposed on it for its own GDPR violations. The Customer remains responsible for controller obligations, including notifications to supervisory authorities and data subjects.