Data Processing Agreement

ChannelDock B.V. | Version 1.2 | 3 November 2026

1. Parties, incorporation and effective date

This Data Processing Agreement (DPA) is between ChannelDock B.V., Dutch Chamber of Commerce number 83335218, Entrada 100, 1114 AA Amsterdam, the Netherlands (ChannelDock), and the customer legal entity that uses the ChannelDock services under ChannelDock's Terms and Conditions, an order form or another service agreement (Customer). Those documents constitute the Agreement.

This DPA forms part of the Agreement from the earliest of: the Customer's acceptance of Terms and Conditions that refer to this DPA, the Customer's signature of this DPA, or other written or recorded electronic acceptance. A signature is not required for the DPA to apply. This DPA is the only data processing agreement between the parties for the services and replaces any earlier one. Data processing terms proposed by the Customer, including in purchase orders, questionnaires or the Customer's own templates, do not apply unless an authorised representative of ChannelDock signs them.

2. Scope and roles

This DPA governs personal data ChannelDock processes on the Customer's behalf to provide its warehouse management, inventory, order, shipping, returns, product information, AI and connected commerce services (Customer Personal Data). The Customer acts as controller, or as processor for its own customers; ChannelDock acts respectively as processor or subprocessor.

Where the Customer is a processor, it warrants that it has the controller's authority for its instructions and for ChannelDock's appointment, it remains ChannelDock's sole point of contact, and it handles all communication with its controllers. ChannelDock has no obligations towards the Customer's controllers or customers except where mandatory law provides otherwise.

The EU GDPR, applicable Member State data protection law, and the UK GDPR and Data Protection Act 2018 where applicable (Data Protection Law) govern the processing. Terms defined in the GDPR have the same meaning in this DPA. The schedules form part of this DPA.

3. Instructions

ChannelDock processes Customer Personal Data only on the Customer's documented instructions, including with regard to transfers, unless law requires otherwise; in that case ChannelDock informs the Customer before processing unless the law prohibits this. The Customer's complete instructions are: the Agreement, this DPA, and the use, settings, integrations and AI features that the Customer and its users choose in the services. Actions of the Customer's users and API or MCP credentials in the account count as the Customer's instructions.

Instructions beyond the standard functionality of the services require ChannelDock's prior written agreement and may be charged under section 13. ChannelDock may decline instructions that are not technically feasible or would require changes to the services. ChannelDock informs the Customer if, in its opinion, an instruction infringes Data Protection Law, and may suspend the affected processing until the Customer confirms or changes the instruction. ChannelDock is not obliged to perform a legal review of instructions.

ChannelDock does not sell Customer Personal Data, does not use it for advertising and does not use it to train general-purpose AI models. ChannelDock may create and use aggregated or anonymised data that no longer identifies any individual, and data about the use of the services, to operate, secure, support and improve the services.

4. Customer responsibilities

The Customer is responsible for: the lawfulness of the processing and its instructions; a lawful basis and the required notices for all Customer Personal Data; the accuracy of the data it submits; the user accounts, permissions, passwords, multi-factor authentication, API keys and MCP credentials of its

account; and the marketplaces, carriers, fulfilment partners, apps, AI tools and other third parties it connects to the services, including through the API or MCP. The Customer shall not submit special-category or criminal-conviction data, or personal data of children, unless ChannelDock has agreed to this in a separate signed document.

The Customer decides whether its users use AI features, and can turn all AI features off for its account (Schedule 3). Output of AI features may be incomplete or inaccurate; the Customer reviews it before relying on it, publishing it or sending it to anyone.

The Customer indemnifies ChannelDock against claims of third parties (including individuals, the Customer's own customers and controllers), fines and orders of supervisory authorities to the extent permitted by law, and reasonable costs including legal fees, to the extent they result from the Customer's breach of this DPA or Data Protection Law, its instructions, or data it submitted without a lawful basis.

ChannelDock's processing of its own account, billing, support, business-contact and security records is not covered by this DPA; ChannelDock is controller for that processing under its Privacy Statement.

5. Confidentiality and security

ChannelDock ensures that persons authorised to process Customer Personal Data are bound by confidentiality, and limits access to personnel who need it to provide, support or secure the services. ChannelDock implements the technical and organisational measures described in Schedule 2. The Customer has reviewed these measures and agrees that they provide a level of security appropriate to the risks of the processing. ChannelDock may change the measures, provided the overall level of protection is not materially reduced. Security of the Customer's own devices, networks, accounts and connected third parties is the Customer's responsibility.

6. Subprocessors and other recipients

The Customer gives ChannelDock general written authorisation to engage subprocessors. The subprocessors in Schedule 3 and the public subprocessor register are approved. ChannelDock imposes on each subprocessor by written contract the data protection obligations required by Article 28(4) GDPR and remains liable to the Customer for the subprocessor's performance of them, subject to section 12.

ChannelDock informs the Customer of an intended addition or replacement of a subprocessor by updating the public register and notifying the account's email address or showing a notice in the portal, at least 10 days before the change. The Customer may object in writing within that period on reasonable, documented data protection grounds. Without a timely objection the change is accepted. After an objection the parties discuss a solution in good faith; for a provider used only for AI features, turning AI features off for the account is such a solution. If no solution is agreed within 30 days of the objection, the Customer may terminate the affected service by written notice without a termination fee. This is the Customer's sole remedy. Where a change is urgently needed for security, continuity or legal reasons, ChannelDock may make it immediately and informs the Customer as soon as practicable; the objection procedure then applies afterwards.

Marketplaces, carriers, fulfilment centres, payment providers, apps, AI tools and other third parties that the Customer connects to or selects in the services receive data on the Customer's instructions. They are not ChannelDock's subprocessors, and ChannelDock is not responsible for their processing.

AI features send the data needed for the feature the Customer's user chooses, such as an uploaded file for column mapping or order data an AI agent retrieves, to the AI providers in Schedule 3 or to ChannelDock's own AI model, which runs on ChannelDock's infrastructure at DigitalOcean. Address recognition during order import sends only street address lines and the country code. ChannelDock uses these providers under terms and settings under which data submitted through their APIs is not used to train their models.

7. Assistance

Taking into account the nature of the processing and the information available to it, ChannelDock assists the Customer with requests from individuals exercising their rights and with the Customer's obligations under Articles 32 to 36 GDPR. This assistance is provided primarily through the functionality of the

services (search, export, correction and deletion) and through this DPA and ChannelDock's documentation. ChannelDock forwards to the Customer, without undue delay, requests from individuals it receives about Customer Personal Data and does not respond to them itself unless law requires it. Further assistance is provided within a reasonable time and may be charged under section 13.

8. Personal data breaches

ChannelDock notifies the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data, with the information reasonably available to it, which it may provide in phases. ChannelDock takes reasonable steps to contain, investigate and mitigate the breach. Unsuccessful attempts and events that do not compromise the security of Customer Personal Data, such as pings, port scans or blocked log-in attempts, are not breaches under this section. A notification is not an acknowledgement of fault or liability.

The Customer decides on and makes notifications to supervisory authorities and individuals, and bears their costs, unless the breach was caused by ChannelDock's breach of this DPA. Breaches caused by the Customer's users, credentials, devices or connected third parties are the Customer's responsibility.

9. International transfers and requests from authorities

The Customer authorises ChannelDock and its subprocessors to process Customer Personal Data outside the European Economic Area and the United Kingdom where needed for the services, provided the transfer complies with Chapter V GDPR, for example through an adequacy decision (including the EU-U.S. Data Privacy Framework for certified providers) or the European Commission's Standard Contractual Clauses, or the UK equivalents, entered into by ChannelDock or its subprocessor. Information about the transfer mechanism of a subprocessor is available on request.

If an authority demands access to Customer Personal Data, ChannelDock informs the Customer unless the law prohibits this, refers the authority to the Customer where possible, and discloses only what it is legally required to disclose. ChannelDock may, but is not required to, challenge such a demand.

10. Return and deletion

The Customer can export its data with the export functions of the services during the term and for 90 days after the services end. After that period ChannelDock deletes Customer Personal Data from its active systems, unless law requires it to retain data. Copies in backups are deleted in the normal backup cycle, within 12 months, and remain protected until then. Shorter periods required by marketplaces, such as for Amazon data, apply automatically. On written request ChannelDock confirms the deletion. Returns or exports in another form than the standard export functions, and deletion instructions that cannot be carried out with the functionality of the services, may be charged under section 13.

11. Information and audits

ChannelDock makes available the information necessary to demonstrate compliance with Article 28 GDPR and allows for and contributes to audits, including inspections, by the Customer or an auditor it mandates, as follows. (a) The Customer first relies on this DPA, ChannelDock's public security information and, on request, written answers to a reasonable security questionnaire and a summary of relevant policies or test results. An audit or inspection may follow only if that information is insufficient to demonstrate compliance. (b) No more than one audit in any 12-month period, with at least 30 days' written notice and an agreed scope, during business hours, remotely where possible, and for no more than one working day. (c) The auditor is independent, bound by confidentiality and not a competitor of ChannelDock; ChannelDock may object to an auditor on reasonable grounds. (d) Audits do not include access to other customers' data, source code, trade secrets, or information that would compromise security or breach obligations to third parties. Subprocessors are audited through their own reports and certifications. (e) The Customer bears its own costs and pays ChannelDock's time at its then-current rates, unless the audit shows that ChannelDock materially breached this DPA. (f) The limits in (b) do not apply where a supervisory authority requires the audit. (g) The results are confidential and are shared with ChannelDock, which addresses any confirmed material non-compliance within a reasonable time.

12. Liability

Each party’s liability arising out of or in connection with this DPA, including under Data Protection Law, is subject to the limitations and exclusions of liability in the Agreement and counts towards, not in addition to, any aggregate limit in the Agreement. ChannelDock is not liable for damage, fines or costs to the extent caused by the Customer’s instructions, the Customer’s breach of this DPA or Data Protection Law, or third parties the Customer connected or selected. A fine imposed on a party by a supervisory authority is borne by that party, unless and to the extent it was caused by the other party’s breach of this DPA. Nothing in this DPA limits liability that cannot be limited under applicable law.

13. Costs

ChannelDock performs its obligations under this DPA within the agreed fees where they are covered by the standard functionality of the services, this DPA and ChannelDock’s public documentation. Other work at the Customer’s request, including individual security questionnaires, assistance under sections 7 and 10, audits under section 11, non-standard exports, and reviewing or negotiating the Customer’s own terms, may be charged at ChannelDock’s then-current hourly rate, which is EUR 95 per hour excluding VAT at the date of this version. ChannelDock gives an estimate before starting work expected to take more than four hours. No charge applies to work required because of ChannelDock’s breach of this DPA.

14. Changes to this DPA

ChannelDock may change this DPA to comply with law or guidance of supervisory authorities, to reflect changes to the services or subprocessors under section 6, or in other ways that do not materially reduce the protection of Customer Personal Data. ChannelDock publishes the new version and notifies the Customer at least 30 days before it takes effect. If a change materially reduces that protection, the Customer may terminate the affected services before the change takes effect. Continued use of the services after that date means acceptance of the new version; a new signature is not required.

15. General

Privacy requests and notices to ChannelDock are sent to legal@channeldock.com. Notices to the Customer are sent to the email address of its account or shown in the portal. If this DPA conflicts with the Agreement, this DPA prevails for data protection matters, except that the limitation of liability in the Agreement applies as set out in section 12. Where Standard Contractual Clauses apply, they prevail for the transfer concerned. Dutch law applies to this DPA, and disputes are submitted exclusively to the competent court in Amsterdam, subject to mandatory law. This DPA ends automatically when ChannelDock no longer processes Customer Personal Data; sections 4, 10, 12 and 13 survive.

Processing & security

Schedule 1. Processing particulars

Element	Description
Subject and purpose	Provision, support and security of ChannelDock’s warehouse management, multichannel commerce, product information and AI services for the Customer.
Nature of processing	Collection through customer input and connected APIs; recording, hosting, organisation, retrieval, synchronisation, order routing, label generation, AI features chosen by the Customer, disclosure to recipients the Customer selects, correction, export and deletion. Ongoing during use of the services, triggered by orders, integrations and user actions.
Individuals	Customer users and staff; buyers, delivery recipients, return requesters, supplier contacts and other business contacts whose details the Customer submits or connects.
Personal data	Names, email addresses, phone numbers, delivery and billing addresses, account and user identifiers, order and shipment references, purchased items, return details, tracking information, messages, IP addresses and access logs.
Sensitive data	Not in scope (section 4). The Customer shall not enter sensitive information in free-text fields.
Duration	The term of the Agreement plus the export and deletion periods in section 10.

Schedule 2. Technical and organisational measures

ChannelDock’s measures include the following, applied in proportion to the risks and updated under section 5:

Access: individual user accounts, role-based permissions and least-privilege access; multi-factor authentication for administrative access to infrastructure; removal of access that is no longer needed; confidentiality obligations and security awareness for personnel.

Infrastructure and encryption: hosting in data centres of certified providers in the EU; TLS for data in transit; encryption at rest; restricted access to secrets and keys; network protection.

Operations: logging of security-relevant events, monitoring, vulnerability and patch management, controlled software changes, and an incident response procedure.

Availability and lifecycle: backups and recovery procedures, automatic anonymisation and deletion periods, and secure deletion of data and media.

Providers & privacy information

Schedule 3. Approved subprocessors

The functions below describe what each provider may be used for; the public register gives current details and locations. A provider acting only for ChannelDock's own controller purposes is outside this DPA.

Provider	Function
DigitalOcean, LLC (including Spaces)	Cloud infrastructure in the EU: servers, databases, object storage and containers, including hosted AI agents and ChannelDock's own AI model.
Amazon Web Services, Inc.	Object storage for files and assets where used.
Cloudflare, Inc.	Network protection and traffic delivery.
Mollie B.V.	Payment processing, to the extent acting as processor.
Sendinblue SAS (Brevo)	Service emails and notifications.
Google Cloud EMEA Limited (Google Workspace)	Email, calendar and documents used for support and account management.
Fireflies.ai Corp.	Recording and notes of support, onboarding and sales calls, where Customer Personal Data is shown or discussed in the call.
Pipedrive OÜ	Customer relationship management, where it contains Customer Personal Data.
Slack Technologies, LLC	Internal operational notifications.
OpenAI Ireland Ltd (OpenAI API)	AI features: the AI assistant, column mapping of uploaded files, product content, translation and image editing; fallback for address recognition.
X.AI LLC (xAI API)	AI features: address recognition during order import, listing quality checks and product content.
Google LLC (Gemini API)	AI features: product image generation and editing; fallback for address recognition.
OpenRouter, Inc.	AI features: language model access for AI agents, forwarding requests to the model provider configured for the agent.
SideGuide Technologies, Inc. (Firecrawl)	AI features: web search and page retrieval for AI agents.

Turning AI off: an admin of the Customer can turn off all AI features for the account in the account's general settings. ChannelDock then sends no data of that account to the AI providers above or to its own AI model, except for address recognition during order import (section 6).

Public information

The following pages are provided for information. They do not create obligations beyond this DPA, and this DPA prevails if they differ.

Privacy Statement	https://channeldock.com/privacy-statement
Data protection and security	https://channeldock.com/data-protection
Subprocessor register	https://channeldock.com/subprocessors/
Terms and Conditions	https://channeldock.com/terms-and-conditions/

Legal references: Regulation (EU) 2016/679, in particular Articles 28, 32-36 and Chapter V; Commission Implementing Decision (EU) 2021/914; UK GDPR and applicable UK transfer instruments.