CONTRACT DOCUMENT

Personal Data Processing Agreement

Shopify service, Annexes A, B and C

AUTHOR	DATE	VERSION
Valeria S.r.l.	31/10/2026	shopify_5.0-en

1. Parties, scope and conclusion of the agreement

This personal data processing agreement (the “DPA”) is concluded between the merchant identified in the service contract and its acceptance (the “Merchant” or “Controller”) and Valeria S.r.l., with its registered office at Via Roma 38/A, 21 018 Sesto Calende (VA), Italy, Tax Code and VAT No. 04 116 360 126 (“Valeria” or the “Processor”).

Under Article 28 of Regulation (EU) 2016/679 (the “GDPR”), the DPA governs Valeria's processing of personal data on behalf of the Merchant to provide the shopping and order support assistant and related Shopify store management services. Annexes A, B and C form an integral part of the agreement and define the processing, security measures and authorised sub-processors.

This DPA, version shopify_5.0-en dated 31/10/2026, is incorporated into the Shopify Terms of Service or concluded through a separate written agreement identifying its version and annexes. The Merchant accepts the DPA and its annexes in writing, including electronically, before processing on its behalf begins, including the management of invitations and operator access permissions. The Parties retain a copy of the agreement and evidence of acceptance. The Merchant may request a copy bearing its details at support@valeria.food.

If the DPA conflicts with the service contract, the DPA takes precedence on personal data protection matters.

The DPA covers the store's visitor and customer data, content used in the service and operator data processed to manage the Merchant's authorisations and activities. Processing for which Valeria acts as an independent controller remains separate: general account authentication and security, management of the commercial relationship, aggregate usage measurement for billing, billing and compliance with legal obligations. Such processing is governed by Valeria's relevant privacy notice.

Where the Merchant activates the Telegram channel, the DPA covers assistance through that channel, the customer's requested link to their store account and management of the associated cart. Independent processing by the Telegram platform is separate and governed by its privacy policy.

For obligations towards Shopify, “Merchant Data” includes information about the Merchant, the store and its customers as defined in the Shopify API Terms.

2. Instructions and obligations of the Parties

Valeria processes personal data only on the Controller's documented instructions, including in relation to transfers. Instructions comprise this DPA, its annexes, the service functions adopted by the Merchant, authorised configurations and written communications from designated contacts. If European Union or national law applicable to Valeria requires different processing, Valeria informs the Controller before proceeding, unless that law prohibits such information on important grounds of public interest.

The Controller determines the purposes of processing and verifies its lawfulness, adopts the data categories and retention periods in Annex A and makes the necessary privacy notices available before activating the service. For the full standard service, the Controller completes its own data protection impact assessment (the “DPIA”) before processing. A different assessment requires the Controller to document and implement a reduced service scope. Valeria provides the assistance

described in Chapter 5; the common documentation provided by Valeria does not replace the Controller's assessment and conclusion.

Valeria immediately informs the Controller if, in its opinion, an instruction infringes the GDPR or other applicable data protection provisions and does not carry out unlawful processing. The Parties clarify or correct the instruction in writing.

Valeria does not use data entrusted by the Controller to train or generally improve artificial intelligence systems or products, create data collections shared between customers, carry out commercial comparisons between stores or pursue other purposes of its own. This prohibition also covers derived or aggregated data and anonymisation undertaken for those purposes. Data reduction and aggregation necessary to provide the service remain subject to the Controller's instructions.

The service does not provide for processing data relating to criminal convictions and offences, clinical documents, medical prescriptions or identity documents, or for automated decisions producing legal or similarly significant effects on data subjects. New purposes or data categories require prior assessment and agreement.

The Merchant selects the documents and web pages to be used for answers and verifies that it may permit their acquisition and use. Permitted sources concern the store, catalogue, FAQs and commercial terms. Public availability of a page does not authorise importing personal data unrelated to those purposes.

3. Confidentiality and security

Valeria permits access to data only by authorised, instructed persons who are bound by confidentiality, to the extent necessary for their assigned activities. It revokes access that is no longer necessary. Support access is authorised and recorded.

Valeria implements the technical and organisational measures in Annex B and verifies their effectiveness before processing personal data in the service environment. It reviews the measures in relation to the risks of processing and communicates material changes directly to the Controller, obtaining prior agreement. Changes must not reduce the level of protection required by Article 32 GDPR.

4. Sub-processors and transfers

The Controller specifically authorises the sub-processors in Annex C solely for the stated activities and data categories. Adding or replacing a provider, or assigning activities outside the authorised scope, requires the Controller's prior written authorisation, including by email. Valeria communicates the provider's identity, assigned activities, affected data, countries of processing and applicable safeguards. The Controller's silence does not constitute authorisation. If authorisation is refused, the proposed provider does not receive the data and the Parties assess a lawful alternative or a limitation of the service.

Valeria concludes agreements with sub-processors imposing data protection obligations equivalent to those in this DPA for the assigned activities. Valeria remains responsible to the Controller for the sub-processors' performance of those obligations and keeps the applicable list and authorisations up to date.

Transfers of data outside the European Economic Area (the “EEA”) are permitted solely within the scope of Annex C, on the basis of a valid mechanism under Chapter V GDPR and the necessary supplementary measures. Changes to countries or safeguards require a new written instruction before processing. On request, Valeria provides information and copies of the relevant safeguards.

For binding requests from public authorities, Valeria verifies their lawfulness, limits disclosure to the data legally required and informs the Controller to the extent permitted by law.

5. Data subject rights, breaches and assistance

The Controller receives requests to exercise rights under Chapter III GDPR, verifies the requester's identity and decides and communicates the response. Valeria forwards requests received on behalf of the Controller without undue delay and assists it, taking account of the nature of processing, through service functions and necessary actions on the Controller's instructions.

Where data is returned through a file exported from the Merchant's management portal, the authorised operator downloads it in a structured, machine-readable format, verifies completion of the download and confirms secure custody. Confirmation initiates deletion of the copy generated by Valeria. The Controller arranges delivery to the data subject. For further returns, the Parties agree on a secure channel; files containing personal data are not sent as ordinary email attachments.

Valeria assists the Controller in complying with Articles 32, 33, 34, 35 and 36 GDPR, taking account of the nature of processing and the information available to it. It provides available information on processing, security measures, providers and risks for DPIAs and any prior consultations with the supervisory authority. The contact address for assistance and communications relating to the DPA is support@valeria.food.

Valeria informs the Controller's contact without undue delay after becoming aware of a personal data breach. It communicates, including progressively, the nature of the breach, the categories and numbers of data and data subjects involved, the likely consequences, measures taken or proposed and a contact for further information. Valeria contains the incident and cooperates in its management. The Controller assesses notifications to the authority and communications to data subjects under Articles 33 and 34 GDPR.

Valeria's obligations towards Shopify apply separately: notification of an actual or suspected compromise of Merchant Data takes place immediately and, in any event, within 24 hours of becoming aware of it.

6. Retention and termination of the service

During provision of the service, the periods in Annex A apply unless a different lawful and practicable written instruction is agreed before processing. Earlier deletion, restriction and other data subject rights remain applicable.

On termination of the service, the Controller chooses return or deletion of personal data. Following return, Valeria deletes the copies remaining in its possession.

For the Shopify service, Valeria deletes originals, copies and reproductions of Merchant Data within 30 days of app uninstallation, the data no longer being necessary for the service or receipt of a binding deletion request from the Merchant, customer or Shopify, whichever applicable event

occurs first. The deadline includes exported files, records, evidence of data subjects' choices and backups. Return, deletion cycles and ordinary retention periods do not extend that deadline.

Further retention is permitted only where required by law. Valeria documents the applicable provision, necessary data and retention duration, limits use and access and informs the Controller where permitted.

Valeria ensures deletion of residual copies and, following restoration from backup, reapplies deletions before reopening the service. It provides confirmation to the Controller. If it cannot meet the deadline applicable to Shopify, it promptly informs Shopify, without that communication releasing it from the obligation to delete.

7. Verification and duration of the agreement

Valeria makes available to the Controller the information necessary to demonstrate compliance with the DPA and allows and contributes to audits and inspections carried out by the Controller or its appointed auditor. Agreed arrangements protect other customers' data and service security without preventing necessary checks or interventions by the supervisory authority.

The DPA remains effective for the full duration of processing, including return and deletion operations. Confidentiality and cooperation obligations and mandatory statutory liabilities remain applicable.

Annex A. Scope of processing and retention

A.1 Subject matter, nature and data subjects

Processing concerns provision of the shopping and order support assistant in the Shopify store and management of integration, configurations, operator authorisations, support, maintenance, security and requests relating to data subject rights.

Operations include receipt, consultation, processing, recording, storage, transmission to authorised providers, export, restriction and deletion of data. Processing takes place according to use of the service and necessary maintenance activities, for the duration of the relationship and within the retention limits below.

Data subjects are the store's visitors and customers, operators authorised by the Merchant and persons who may appear in business documents permitted in the service. Data associated with codes replacing names or other direct identifiers remains personal data where it can be linked to a person.

A.2 Data categories and purposes

Activity	Personal data and purposes
Shopping assistance	Customer messages, assistant and operator responses, feedback, conversation and customer identifiers, language, products and cart quantities, to respond to requests and rank products according to the context. For authenticated customers, a link to the store account and consultation of first and last names by authorised operators, to recognise customers and provide assistance. The Telegram channel also processes user, chat and message identifiers, the link to the store account, cart state and recorded operations, to recognise the customer, apply their choices and continue purchases. The IP address is processed transiently for catalogue queries.
Memory across conversations	Preferences and relevant information supplied by the customer, to personalise assistance in subsequent conversations.
Personalisation and order support	Customer order identifiers and numbers, dates, products and variants, product codes, quantities, prices, discounts, taxes, amounts and currency; payment, cancellation, fulfilment and shipment status; carriers, tracking codes and links, estimated or actual shipping and delivery dates, returns and refunds, where available. Consultation serves to tailor suggestions and responses to the customer's purchases and answer questions about their orders. Customer addresses, contact details, card numbers, security codes and financial credentials are not requested.
Measurement of purchases following chat	Identifiers linked to the customer, dates, status, amounts, currency and information necessary to connect orders with interactions with the assistant. Order data is examined before such connections are identified; individual results are retained only while consent is active, without product details, addresses or payment credentials.
Health information, images and dictation	Health information relevant to the request, permitted images, thumbnails, transient audio and transcribed text, to support the interaction methods requested by the customer. Intentional use of health data requires separate explicit consent; remembering it also requires consent to memory.
Usage statistics and diagnostics	Usage events, counters, feedback and content necessary for diagnostics, to measure, provide and correct the service on behalf of the Merchant.
Operator management and business documentation	Invitations, permissions, roles, configurations and records of operator activities; support request notifications, operator contact details and preferences, and reading and sending records; documents and web pages selected by the Merchant, source addresses, extracted text, excerpts, numerical representations for search and related copies and versions, to administer the service and make the Merchant's information available. Personnel records and customer lists are excluded.
Rights and evidence of choices	Controller and data subject identifiers, right exercised, dates, request status and outcome, exported files, privacy choices and text versions, to manage rights and document choices. The request register does not retain the full text of requests or identity documents.

Memory, personalisation and order support, and measurement of purchases following chat are restricted to authenticated customers, off by default and subject to separate withdrawable consents. Consent to personalisation and order support covers both uses of orders described in the table. Refusal or withdrawal does not prevent essential chat.

Order consultation is restricted to the store and the customer's verified account. It covers Shopify orders from the last 60 days, including searches by identifier, and is subject to the integration's permissions. It does not modify orders or carry out cancellations, returns or refunds. Withdrawal of the relevant consent stops consultation and closes the current conversation; orders retained by the Merchant remain unchanged.

During human support, the original customer and operator messages are retained in the conversation history. When the conversation returns to the assistant, the authorised AI provider processes the content to identify and mask personal identifiers and health information in the copy used to continue the chat. These checks do not anonymise the history and may fail to identify some data. First and last names consulted at the store are not retained in a separate customer profile archive or included in the assistant's context.

A.3 Limits concerning health data

Before activating processing that may involve health data, the Parties document the applicable legal basis and, where necessary, the condition under Article 9 GDPR. In automated assistance, if a customer sends health content without giving the relevant consent, text, images and transcribed content may be processed transiently to identify it and prevent unauthorised use. These automated controls may not recognise every item of content. Withdrawal of health consent entails removal of remembered health information.

Voluntary disclosure of health information during human support does not, by itself, constitute explicit consent to its use. The Merchant limits requests to data necessary for assistance and, when it identifies excessive content without an applicable legal basis, arranges its deletion with Valeria's assistance. The ordinary retention period for conversations does not justify keeping such content.

Consent to personalisation and order support does not automatically cover health data that may be inferred from the products purchased. Before such use, the Controller assesses health consent and necessary controls in the DPIA. For functions concerning food or allergens, the Controller adopts relevant sources, rules, notices and safety checks.

Images whose main subject is an identifiable person and continuous voice conversation are excluded.

A.4 Retention periods during the service

Data	Retention period
Conversations with the assistant and operators, feedback, thumbnails and the link to the authenticated customer	90 days from the close of the conversation.
Original or resized images	Deletion on completion of the answer; images prepared but not linked to a conversation are deleted after 48 hours.

Data	Retention period
Audio	Not retained by Valeria or the transcription provider. Copies held on Telegram are governed separately.
Orders consulted for personalisation and support	No separate archive of the consulted orders is retained. Data included in the conversation or diagnostics follows the corresponding periods. The 60-day limit concerns orders accessible through Shopify, not retention of the data obtained.
Carts managed through the channel and related operations	90 days from the cart's last update. Where an operation has an unresolved outcome, content is deleted and only identifiers and states necessary to prevent duplication remain until resolution or erasure of the customer's or store's data.
Links between Telegram and store accounts	While active, until revocation or erasure; revoked links and expired linking requests are deleted after 90 days from revocation or expiry. Disabling the channel alone does not revoke the link.
Customer memories and settings	Until withdrawal, deletion or 365 days of inactivity.
Measurement, usage, assisted orders and records of operator activities	730 days from the event, day of use, order completion or recording of the activity.
Support notifications and reading and sending records	90 days from creation of the alert, unless deleted earlier. Communication and language preferences remain until the account or organisation is deleted; disabling email removes the contact address associated with the preference.
Diagnostics and application records	30 days from recording.
Documents, web pages and derived content for answers	Until removal or termination of the service; superseded versions are retained for 90 days. The same periods apply to copies of acquired content, excerpts and search indexes.
Exported files	Deletion is initiated after confirmation of secure custody; removal takes place within 30 days of generation.
Evidence of choices and rights requests	Current choices are retained while active; related evidence for 5 years from replacement or withdrawal. Essential data on closed requests is retained for 5 years from closure.
Service backups	Automatic deletion of copies more than 14 days old, according to the execution cycle of the applicable rule. Copies are reserved for restoration.
Restore copies of Microsoft-managed databases, where used	Ordinary retention not exceeding 35 days, exclusively for restoration.
Any request and answer archives held by the AI processing provider	30 days, where used to ensure continuity of processing.

Data	Retention period
Infrastructure and provider records relating to the Controller's data	Deletion within 30 days of recording. Before entrusting data, Valeria verifies that the provider's services are compatible with that deadline.

Evidence of choices and rights requests is not reused for conversations, personalisation or service measurement. The five-year period does not constitute an independent legal basis. Any processing for Valeria's own purposes concerns only the essential data necessary for its obligations or for establishing or defending a right, excluding conversation content, exported files, documents and health data.

Content entrusted to AI processing services may be subject to the provider's security controls, including review of flagged content. Before entrusting data, Valeria verifies that the conditions and periods applicable to those controls are compatible with the Controller's instructions and this DPA.

All periods are subject to earlier deletion and the deadlines in Chapter 6, including data retained by providers and restore copies.

Annex B. Technical and organisational measures

Valeria implements and verifies the following measures before processing personal data in the service environment.

Area	Measures
Access and separation of data	Named accounts, permissions limited to necessary activities, multi-factor authentication for privileged access and revocation of access no longer needed. Service checks limit access to data relating to the authorised organisation, store and customer. Support access is recorded.
Encryption and credentials	Encryption of data during transmission and in storage, including databases, exported files and backups. Access to keys is limited to authorised persons; credentials used to connect the service to the Merchant's systems are protected and revoked where necessary.
Data reduction and data subject choices	Collection of only necessary data, verification of privacy choices before using functions that depend on them, checks on incoming content and application of withdrawals and deletions. Access to diagnostic data is restricted to authorised persons.
Continuity and deletion	Backups separated from operational storage, defined retention periods and restoration checks. Deletions are reapplied following restoration and deletion deadlines also cover copies.
Service management and authorised persons	Risk-based vulnerability and update management, monitoring, incident management and verification of the effectiveness of measures. Authorised persons receive instructions and are bound by confidentiality; providers are bound by data protection agreements.

Annex C. Authorised sub-processors and data locations

C.1 Scope of authorisation

The Controller authorises the following providers exclusively for the stated activities and the Annex A data necessary for those activities. Authorisation also covers service administration functions performed on its behalf and does not extend to other services offered by the same provider.

Hosting and ordinary storage of service records, including backup copies, take place in the EEA. Artificial intelligence processing takes place in the European data zone defined by Microsoft, comprising the European Union and the EFTA countries included in that zone. These locations do not exclude access or further processing outside the EEA as described below.

Valeria informs the Controller in writing of the provider actually used, the country and applicable safeguards before entrusting data. Use of an activity already authorised within the limits of this annex does not require new authorisation. Changes outside those limits follow Chapter 4.

C.2 Microsoft Srl

Microsoft Srl, Microsoft House, Viale Pasubio 21, 20 154 Milano, Italy. Data protection contact: Microsoft Privacy.

Authorised activities are application and database hosting, storage of files, copies of acquired content and backups, artificial intelligence processing of content necessary for the service, including generation of numerical representations for searching documents and web pages, audio transcription and sending service notifications to operators about support requests through Exchange Online. These emails contain a link to the conversation, accessible only after authentication and authorisation, without the chat text or customer name. Microsoft receives only the Annex A data necessary for the function used.

The Microsoft Customer Agreement and Products and Services Data Protection Addendum dated 22/05/2026 apply. The application's remote storage, including backups, and the transcription service are located in Italy; data retained by the provider for artificial intelligence functions is located in Sweden, with content processing in the European data zone defined by Microsoft, comprising the European Union and the EFTA countries included in that zone. Other authorised hosting and storage activities remain limited to the EEA as stated in C.1.

Provision may involve access from other countries and the use of further Microsoft sub-processors, including entities in the United States. Such access and transfers must be communicated to the Controller in advance and covered by safeguards under Chapter V GDPR, including, where applicable, the standard contractual clauses adopted by Decision (EU) 2021/914 and necessary supplementary measures.

C.3 Hetzner Online GmbH

Hetzner Online GmbH, Industriestr. 25, 91 710 Gunzenhausen, Germany. Contact: info@hetzner.com.

Authorised activities are hosting the application, databases and storage containing the Annex A data. Ordinary provision is limited to the EEA; for servers located in the European Union, processing and support also take place in the European Union under DPA v1.2 concluded on 07/09/2026. Any separate backup and processing services provided by Microsoft are governed by C.2.

C.4 Cloudflare, Inc.

Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94 107, United States. Data protection officer contact: legal@cloudflare.com.

Authorised activities are distribution and protection of network traffic and protection of access to the service. Processing covers transmitted data necessary for those activities, technical and security data and, where applicable, data used to control access.

DPA v6.4 dated 03/04/2026 applies. Cloudflare uses a global network that may involve processing outside the EEA, including in the United States. Applicable safeguards are the standard contractual clauses under Decision (EU) 2021/914, Module 3 for transfers between processors, and adequacy decisions where applicable, with necessary supplementary measures.

C.5 Further entities and verification of conditions

Before entrusting data to a provider, Valeria verifies that the contract and service arrangements allow compliance with this DPA, including retention and deletion periods. Otherwise, it does not entrust data to the service concerned.

Valeria communicates to the Controller in advance the identity, address, contact, activities and countries of further sub-processors involved in processing and keeps that information up to date and available. The authorisations in Chapter 4 apply; a change to a list published by a provider does not constitute the Controller's authorisation.

Shopify operates within the relationship between the Merchant and its own platform and is not a sub-processor appointed by Valeria under this DPA.

Where the Merchant activates the channel, Telegram Messenger Inc. receives data necessary for communication and acts as an independent controller for its platform under the Telegram Privacy Policy (https://telegram.org/privacy). Telegram is not a sub-processor appointed by Valeria under this DPA. Telegram's retention of messages and attachments, including audio and images, and any transfers outside the EEA follow its own terms. Deletion in Valeria's systems does not delete copies held on Telegram.