Orderlion GmbH

Data Processing Agreement (DPA)

Version 2.2 · Effective 1 October 2026 · Orderlion GmbH

This Data Processing Agreement ("DPA") forms part of the agreement between **Orderlion GmbH**, Himmelpfortgasse 17/7, 1010 Vienna, Austria ("**Orderlion**", the processor) and the customer identified in the Order Form ("**Customer**", the controller) for the Orderlion platform (the "Agreement"). It is concluded in electronic form (Art 28(9) GDPR) by incorporation into the Agreement per the Order Form and Section 12 of the GTC. For the subject matter of data protection, this DPA prevails over the GTC.

1. Roles and scope

1.1 For the personal data processed on the platform on the Customer's behalf (in particular data of the Customer's buyers and their staff, order data, communications and email content processed via Inbox: together "**Customer Personal Data**", described in Annex 1), the Customer is controller and Orderlion is processor.

1.2 This DPA does not apply where Orderlion is itself controller (e.g. contact data of the Customer's staff for account management, billing and support, and pseudonymised usage data for product analytics under Section 3.5); that processing is described in Orderlion's Privacy Policy.

2. Description of the processing

Subject matter, duration, nature and purpose of the processing, types of personal data and categories of data subjects are set out in **Annex 1**.

3. Instructions

3.1 Orderlion processes Customer Personal Data only on the Customer's documented instructions, including with regard to transfers to third countries, unless required to process by Union or Member State law; in that case Orderlion informs the Customer of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.

3.2 The documented instructions consist of: this DPA, the Agreement, the Customer's configuration of the platform (including the chosen Inbox processing mode and the EU-hosting option), and additional instructions in text form. Instructions requiring services beyond the Agreement's scope may be charged at Orderlion's standard rates.

3.3 Orderlion informs the Customer without undue delay if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions, and may suspend execution of that instruction until it is confirmed or modified.

3.4 The Customer instructs and authorises Orderlion to create aggregated, anonymised statistics from Customer Personal Data for product improvement, provided the results contain no personal data and do not identify the Customer, its users or its buyers. Anonymisation is performed as part of this instruction.

3.5 **Product analytics.** Orderlion further processes pseudonymised usage data of platform users (a pseudonymous user identifier together with feature usage, interaction events and device information; not names, contact details, order contents or email content) as an independent controller to improve, secure and develop its services, as described in its Privacy Policy; Section 1.2 applies. Orderlion does not disclose such usage data to third parties other than its own

processors, does not use it to advertise to the Customer's buyers, and deletes or anonymises it at the latest 2 years after collection.

4. Confidentiality

Orderlion ensures that all persons authorised to process Customer Personal Data are bound by contractual or statutory confidentiality obligations, which survive the end of their engagement.

5. Security of processing

Orderlion implements and maintains the technical and organisational measures set out in **Annex 3** (Art 32 GDPR). Orderlion may update these measures provided the overall security level is not materially reduced.

6. Subprocessors

6.1 The Customer grants a general written authorisation for the engagement of the subprocessors listed in **Annex 2**. The current subprocessor list is published at www.orderlion.com/subprocessors and shows the date on which it was last updated.

6.2 Orderlion informs the Customer of any intended addition or replacement of subprocessors at least **30 days** before engagement, by email to the Customer's designated contact and by updating the published list. The notice contains the information needed to assess the change.

6.3 The Customer may object within the notice period on reasonable data-protection grounds, in text form. In that case the parties first seek a solution in good faith (including technical alternatives that avoid the new subprocessor for the Customer's data). If no solution is found within 30 days of the objection, the Customer may terminate the affected services with pro-rata reimbursement of prepaid fees for the terminated services; this is the exclusive remedy for a subprocessor objection. If the Customer does not object within the notice period, the change is deemed approved.

6.4 Orderlion imposes on every subprocessor, by contract, data protection obligations that are in substance the same as those in this DPA, in particular sufficient guarantees of appropriate technical and organisational measures. On request, Orderlion provides the Customer with a copy of the relevant subprocessor terms (redacted for business secrets). Orderlion remains fully liable to the Customer for the performance of its subprocessors' data protection obligations.

7. AI processing

7.1 The Inbox feature and other AI features process Customer Personal Data using large language models of the AI subprocessors named in Annex 2, including each provider's hosting region and retention configuration.

7.2 **No training.** Orderlion does not use Customer Personal Data to train, fine-tune or improve machine-learning models available beyond the Customer's own account, and contractually ensures that its AI subprocessors do not use Customer Personal Data transmitted through Orderlion for training their models.

7.3 **EU-hosted AI option.** On the Customer's written request during setup, confirmed by Orderlion, AI processing for the Customer's account is performed exclusively on EU-located infrastructure. For those accounts, order extraction runs on Anthropic Claude models provided via AWS Bedrock in the EU (Frankfurt), and OpenAI is not used. Annex 2 identifies the processing chain applicable to this option.

7.4 **Provider retention.** The AI subprocessors retain transmitted content only per the retention configurations stated in Annex 2.

7.5 AI outputs are extractions and suggestions subject to the review mechanisms described in the Agreement; the platform makes no decisions based solely on automated processing that produce legal effects concerning data subjects (Art 22 GDPR).

8. Data subject rights

Orderlion forwards to the Customer, without undue delay, any data subject request it receives relating to Customer Personal Data, and does not respond to it except as instructed. Taking into account the nature of the processing, Orderlion assists the Customer with appropriate technical and organisational measures (including export, correction and deletion functions of the platform) in fulfilling requests under Chapter III GDPR.

9. Personal data breach

9.1 Orderlion notifies the Customer of a personal data breach affecting Customer Personal Data **without undue delay, at the latest within 72 hours of becoming aware of it**.

9.2 The notification describes, as far as known: the nature of the breach (where possible: categories and approximate numbers of data subjects and records concerned), a contact point, the likely consequences, and the measures taken or proposed. Information may be provided in phases without undue delay as it becomes available.

9.3 The assessment of risk and any notifications to supervisory authorities (Art 33) and data subjects (Art 34) are the Customer's responsibility; Orderlion provides reasonable cooperation and does not notify authorities or data subjects on the Customer's behalf unless separately agreed.

10. Assistance (Art 32-36 GDPR)

Taking into account the nature of the processing and the information available to it, Orderlion assists the Customer in ensuring compliance with Arts 32-36 GDPR (security, breach notifications, data protection impact assessments, prior consultation). Support that goes substantially beyond the information available from this DPA, its annexes and the published documentation may be charged at Orderlion's standard rates.

11. Demonstration of compliance and audits

11.1 Orderlion makes available the information necessary to demonstrate compliance with Art 28 GDPR: this DPA and its annexes, the current TOMs, and written answers to reasonable audit questionnaires (under confidentiality).

11.2 Where this information is insufficient to demonstrate compliance, or where an audit is required by a supervisory authority or follows a personal data breach affecting the Customer, the Customer (or an independent auditor mandated by it, not a competitor of Orderlion) may conduct an audit, including an inspection at Orderlion's premises: at most once per 12 months, with at least 30 days' notice, during business hours, under confidentiality, and without unreasonable interference with operations. Each party bears its own costs; if the audit reveals material non-compliance, Orderlion bears the Customer's reasonable audit costs.

12. International transfers

12.1 Customer Personal Data is hosted in production on infrastructure in the EU (AWS Frankfurt). Transfers to subprocessors outside the EU/EEA occur only as documented in Annex 2 and only with a valid transfer mechanism under Chapter V GDPR: an adequacy decision (including the EU-US Data Privacy Framework for certified recipients)

or Standard Contractual Clauses (2021/914, Module 3) concluded by Orderlion with the subprocessor, with supplementary measures where required.

12.2 If a transfer mechanism relied on ceases to be valid (e.g. invalidation of an adequacy decision), Orderlion implements an alternative valid mechanism without undue delay; SCCs serve as fallback for Data Privacy Framework-certified recipients.

12.3 The Customer's authorisation of the transfers documented in Annex 2 constitutes its documented instruction with regard to transfers (Art 28(3)(a) GDPR).

13. Return and deletion

13.1 For **30 days** after the end of the Agreement, the Customer can export Customer Personal Data in standard formats via the platform or, on request, with Orderlion's assistance.

13.2 After the export period, Orderlion deletes Customer Personal Data from its active systems, completed at the latest **90 days** after the end of the Agreement, unless Union or Member State law requires storage. Data in backup systems is not actively deleted but expires with the regular backup rotation, at the latest 30 days after deletion from active systems; until expiry it remains protected by the measures in Annex 3, is not restored to active use, and if a restore of other data reproduces deleted Customer Personal Data, the deletion is re-executed.

13.3 On request, Orderlion confirms deletion in writing (scope: completion in active systems and the backup expiry schedule).

14. Liability

The liability regime of the Agreement (GTC Section 10) applies to claims between the parties under or in connection with this DPA. Statutory liability towards data subjects (Art 82 GDPR) and Orderlion's full liability for its subprocessors (Section 6.4) remain unaffected.

15. Term and changes

15.1 This DPA applies as long as Orderlion processes Customer Personal Data and survives the end of the Agreement until deletion is completed under Section 13.

15.2 Changes to this DPA follow the mechanism of GTC Section 1.4; subprocessor changes follow Section 6 of this DPA. Previous versions of this DPA remain available at www.orderlion.com/dpa.

15.3 Austrian law applies as per the Agreement; place of jurisdiction as per the Agreement.

Annex 1 - Description of the processing

1. Subject matter. Provision and operation of the Orderlion platform for the Customer: a multi-tenant cloud ordering platform through which the Customer's business buyers place orders, which are captured, structured and handed over to the Customer's own ERP system, together with the associated communication, notification, authentication, monitoring and AI-supported extraction functions.

2. Duration. For the term of the Agreement. On termination, the return and deletion timeline in Section 13 of this DPA applies and prevails over the retention periods stated below.

3. Nature and purpose of the processing.

Processing activity	Nature and purpose	Personal data processed	Data subjects	Retention during the term
Inbox: receipt of order messages	Receipt and storage of buyer order messages forwarded by the Customer to its Orderlion Inbox address. Receipt is handled by Mailgun or AWS SES, which deliver to Orderlion by webhook.	Sender and recipient email addresses; subject; message body; attachments; voice and audio files for voicemail orders; email metadata	Buyer users and their staff	Raw message content: 90 days where the message contains an order, 30 days where it does not
Inbox: AI-supported order extraction	Conversion of message content into structured order data. Content is transmitted by API to the contracted AI providers named in Annex 2 and processed against Orderlion's predefined prompts. Voice messages are transcribed on EU infrastructure before extraction.	Plain text of message body and attachments, including any personal data the sender has included; audio transcripts; extracted order fields	Buyer users and their staff	As above
AI assistant, reports and recommendations	Answering business questions on the Customer's own platform data, generating automated reports for the Customer's staff, and producing product recommendation campaigns. Advisory output only.	User identifiers; order history and platform data required per feature; questions submitted and answers generated	Buyer users, Customer's staff	1 year
Order creation and processing	Recording and processing of orders placed on the platform and handover of confirmed orders to the Customer's ERP system.	Buyer user identifier; customer reference; order lines (items, quantities, prices); order date and time; delivery details; identifier of the Customer's staff member who created the order, where an order is placed on a buyer's behalf	Buyer users, Customer's staff	2 years, after which the link between the order record and the ordering user is removed
Checkout and payment recording	Recording of in-platform order payments for the Customer's records and for display to the Customer and the buyer.	Buyer user identifier; total payment amount; payment status; timestamps. Card and bank credentials are processed exclusively by the payment provider and are not stored by Orderlion.	Buyer users	2 years
Buyer user invitation, signup and onboarding	Invitation of buyer users by the Customer and creation of their accounts, to enable login, account assignment and attribution of placed orders. Invitations are always triggered by the Customer and are sent by email and, where the Customer provides a mobile number, by SMS. By default the SMS contains the invitation link, the invitation code and the Customer's name. The Customer may amend the message and is responsible for any further content it includes.	Name (optional); work email address; mobile telephone number where used for the invitation; invitation reference; assignment to the Customer's account	Buyer users	1 year after last activity

Processing activity	Nature and purpose	Personal data processed	Data subjects	Retention during the term
Authentication and access control	Verification of user identity at login and restriction of access to the data each user is authorised to see.	Email address; salted password hash; login timestamps; session identifiers	Buyer users, Customer's staff	1 year after last activity
In-platform messaging	Provision of messaging between the Customer's staff and its buyer users, including delivery of message notifications.	Sender and recipient user identifiers; message text and attachments; timestamps; notification delivery metadata	Buyer users, Customer's staff	1 year
Transactional notifications	Dispatch of transactional notifications such as order confirmations and status updates, by email and mobile push notification, on the Customer's behalf.	Recipient name and email address or device push token; notification content; dispatch timestamps	Buyer users, Customer's staff	4 weeks
Security monitoring (access control layer)	Logging of security-relevant user actions in the platform's internal access control layer, in particular destructive or permission-changing actions, to ensure traceability and support investigation of security incidents.	User identifier; action type and target object; timestamp; technical metadata including IP address and session	Buyer users, Customer's staff	1 year
Assistance with data subject rights requests	Processing of requests under Articles 12 to 23 GDPR relating to platform data, including identity verification, fulfilment and documentation of the outcome as evidence of compliance.	Requester identity and contact details; verification data; request content; outcome documentation and correspondence	Buyer users, Customer's staff	1 year after last activity

4. Types of personal data. Identification and contact data (name, work email address, and mobile telephone number where used for buyer invitations); account and login data (credentials in hashed form, roles, permissions, session data); order and transaction data; message and email content and metadata, including attachments and voice messages processed through the Inbox; technical data (IP address, device and browser information, timestamps).

5. Categories of data subjects. Buyer users and their staff, meaning employees of the Customer's own business customers; the Customer's staff using the platform.

6. Special categories of personal data. None intended, and no function is designed to collect them. Because the content of messages processed through the Inbox is determined by the sender and cannot be filtered in advance, such content may incidentally contain personal data that the sender chose to include.

7. Frequency of processing. Continuous for the duration of the Agreement.

Annex 2 - Subprocessors

Lists only subprocessors that process Customer Personal Data on Orderlion's behalf. Vendors used solely for Orderlion's own internal operations are not subprocessors under this DPA and are not listed. Where an integration middleware or EDI provider is contracted by the Customer rather than by Orderlion, that provider is the Customer's own processor and is not listed here; where Orderlion contracts one, it is listed and marked as applying only to those accounts whose integration uses it.

The subprocessors engaged by Orderlion are set out in the subprocessor list published at www.orderlion.com/subprocessors. That list forms part of this DPA, and the version published on the effective date of this DPA is the list authorised under Section 6.1. The list states the date on which it was last updated and records its own change history.

The list is published separately rather than reproduced here so that it stays current. Adding or replacing a subprocessor is not an amendment to this DPA: it follows Section 6, under which Orderlion gives at least 30 days' notice before engagement and the Customer may object on reasonable data-protection grounds within that period.

On request, Orderlion provides the list as it stood on a given date as a dated PDF, for customers who need a record of the subprocessors authorised at the time of signature.

Annex 3 - Technical and organisational measures (Art 32 GDPR)

Contains only measures that are in place and have been reviewed and confirmed. Measures that are planned or under remediation are deliberately not listed here; Orderlion discloses those separately in its Security Overview rather than presenting them as operating controls.

1. Pseudonymisation and encryption (Art 32(1)(a))

Encryption at rest. All Customer Personal Data is encrypted at rest with AES-256. The application database on MongoDB Atlas and the AWS storage used by the platform apply provider-side encryption automatically, covering live data, snapshots and backups. Key management is operated by the infrastructure providers under their certified programmes; no customer-managed key option is offered.

Encryption in transit. All traffic between clients, meaning browser, mobile applications and API consumers, and Orderlion's servers is encrypted using TLS. Legacy SSL protocols are disabled. File exchange with customer systems uses FTPS or SFTP.

Credential protection. User login passwords are stored salted and hashed with bcrypt and never in plain text. Internal service credentials are stored encrypted with AES-256.

2. Confidentiality and access control (Art 32(1)(b))

Tenant segregation. Customer data is logically segregated per tenant, and segregation is enforced by the platform's authorisation layer on every request.

Individual accounts. Staff and contractors use individual, personally attributable accounts on every system that contains personal data or provides security-relevant access. Shared credentials are prohibited for those systems. Where a credential genuinely has to be used by more than one person, it is distributed through a permission group in the company password manager, so that who can retrieve it is controlled and reviewable. Such a credential is a shared login: actions taken with it are not attributable to an individual, and it is rotated when a member of the group leaves or changes role.

Password policy and password manager. A company password manager (NordPass Business, EU data residency) is mandatory for all staff and contractors and is accessed through Google Workspace single sign-on. Stored credentials require a minimum strength of 20 characters with a complex structure and are changed at least annually. Disabling the Workspace account at offboarding revokes access to all stored credentials automatically.

Multi-factor authentication. MFA is mandatory on business-critical systems, including the Google Workspace identity provider through which the password manager is reached. Account recovery is restricted to executive level.

Least privilege. Access follows a role-based model limited to operational necessity, in which destructive actions are restricted to the highest privilege level and suppliers administer users only within their own account.

Impersonation controls. Impersonation of a customer user is treated as sensitive access. It is restricted to partner management and approved technical personnel, permitted only where operationally necessary for troubleshooting, onboarding, migration or a customer request, and prohibited for any non-business purpose.

Access reviews. Access rights are reviewed quarterly across production and cloud infrastructure, administrative accounts, code repositories, support and analytics systems, contractor access and stale accounts. Each review is recorded.

Network protection. Host firewalls and cloud security groups are configured closed by default, with only the ports required for operation open. Applications run in containers on stateless hosts behind load balancers.

Server access. Server access is limited to named individuals and runs primarily through AWS Systems Manager rather than distributed SSH keys. Where SSH keys are used, they are held by the CTO and Head of Engineering only.

Device security. Company-managed devices are the default for all work and require a strong unlock method, disk encryption, automatic screen locking, current operating system updates, and remote lock or wipe where technically possible. Personal devices may be used only for communication and internal documentation tools, and never for customer or platform data, database, production or infrastructure access, HR or payroll systems, or data exports.

Offboarding. Access is revoked under a documented offboarding checklist: identity provider account disabled, SaaS, cloud, repository and communication access removed, devices recovered and credentials rotated where necessary. Because the company password manager authenticates through Google Workspace single sign-on, disabling the Workspace account revokes access to all stored credentials automatically rather than as a separate manual step.

Email authenticity. Sending domains are protected with SPF, DKIM and DMARC.

3. Integrity, availability and resilience (Art 32(1)(b))

Hosting. All production systems and the application database run on Amazon Web Services in the Frankfurt region (eu-central-1), Germany. Physical data centre security, environmental controls and network-layer protections including distributed denial of service mitigation are provided by AWS under its own certified programme.

Resilience. Application servers are stateless, with automated health checks every 30 seconds and automatic restart of unhealthy instances. Capacity changes are made manually.

Availability. The contractual availability target is 99% per calendar month, excluding announced maintenance and circumstances outside Orderlion's control. Availability is monitored continuously.

Backup. Two backup systems run in parallel. Critical database collections are backed up daily to a secure, encrypted remote location and retained for 30 days, and imported customer and price data is backed up weekly. Separately, the database provider takes its own snapshots, held within the EU and retained for 7 days. Both expire automatically, so data deleted from active systems disappears from all backups within 30 days at the latest.

Recovery objectives. A recovery time objective of 8 hours, being the maximum time to restore service after an incident, and a recovery point objective of 24 hours, being the maximum tolerable data-loss window, aligned with the daily backup cycle.

4. Logging and monitoring

Infrastructure and application monitoring. Server-side monitoring covers health, performance and anomaly alerting, with error tracking on both server and client side. The senior team is alerted to unplanned events, including outside business hours and at weekends.

Platform audit trail. An internal access control layer records security-relevant user actions on the platform, in particular destructive or permission-changing actions such as deactivating buyers or products, so that such actions remain traceable.

Brute-force protection. SSH login attempts are logged and suspicious source addresses are blocked automatically.

Log retention and access. Retention differs by tool: infrastructure and application logs are retained for 14 days, error events for 30 to 90 days depending on the data type, and server logs for a maximum of 30 days. Access is restricted to authorised engineering staff, and logs are not shared with third parties or with individual customers, because they may contain data relating to more than one tenant.

5. Secure development

Four-eyes principle. Every change intended for production is reviewed and approved by at least one further developer before release.

Automated testing. More than 2,000 automated unit and integration tests run on every deployment, end-to-end tests run weekly, and manual quality assurance precedes major releases.

Environment separation. Production, staging and development environments are separated.

Dependency and vulnerability scanning. Automated dependency and vulnerability scanning runs against the code repositories, so known vulnerabilities in third-party packages are surfaced for remediation.

6. Safeguards specific to AI processing

Order extraction uses large language models accessed by API from the providers named in Annex 2, under data processing agreements. Voice messages are transcribed on EU infrastructure before extraction. Providers are contractually barred from training their models on Customer Personal Data transmitted through Orderlion. Platform data is stored in the EU, and AI processing can be restricted to EU-hosted infrastructure on request. Uncertain or anomalous extractions are flagged for human review, and the Customer chooses whether every extracted order is reviewed before transfer to its ERP system.

7. Organisational measures

Policy framework. A written internal compliance and security policy governs identity and authentication, device security, approved tooling, access control, customer data handling and classification, AI usage, vendor management, incident response, and onboarding and offboarding. It is reviewed at least annually and forms part of every employment and contractor relationship.

Incident response. Incidents are detected through monitoring, classified by severity, escalated to the CTO, Engineering Lead and CEO, contained, analysed for root cause and closed with a post-mortem. Personal data breaches follow an additional documented GDPR procedure: every breach is recorded in a breach register, and where Orderlion acts as processor, affected customers are notified without undue delay and at the latest within 72 hours of awareness, or within any shorter period agreed in the individual contract.

Security awareness training. New joiners receive security and data protection onboarding within their first two weeks, covering phishing, password hygiene and the password manager, customer data handling, incident reporting and the rules for AI tools, based on a documented curriculum. A refresher is mandatory for all staff annually, with role-specific sessions for engineering and for commercial teams. Attendance is recorded and coverage is verified quarterly against the current staff list.

Vendor management. Before a new vendor is adopted, a documented review covers the data to be shared, authentication and single sign-on support, availability of a data processing agreement, EU hosting, business criticality and security risk. Vendors processing personal data are recorded in a subprocessor register with their transfer mechanism and agreement status.

Physical security. Office access is secured with physical keys under a key register that logs every key issued and returned, so key holders remain traceable. The office is kept locked at all times, and physical documents containing personal data are stored in locked cabinets.