PAGESEAL · VERSION 2026-11-04

Data Processing Agreement

under Article 28 GDPR, including the service provider terms of the California Consumer Privacy Act

between

> **The merchant who installs Pageseal, with the company details and Shopify store recorded in Pageseal**
> Company, address and Shopify store: _____

– the “Controller” –

and

> **Orbita Media GmbH**
> Ericusspitze 4, 20457 Hamburg, Germany
> Amtsgericht Hamburg, HRB 161613, represented by its managing directors Noah Malik and Stefan Schott
> Email: support@pageseal.app

– the “Processor” –

Applies to every merchant who installs Pageseal, from the time of installation. Concluded in electronic form (Article 28(9) GDPR); no signature is needed. A copy with your company details is available in Pageseal under Settings.

1. Subject matter, duration and conclusion

1.1 The Processor provides the Shopify app Pageseal (the “Service”): checking EPUB files, creating personalised eBook copies for the Controller’s buyers, delivering them by download link and email, and matching shared copies to orders.

1.2 This agreement applies as long as the Controller has Pageseal installed, and afterwards until all data is deleted under section 9.

1.3 The Processor offers this agreement to every merchant who uses the Service. It becomes part of the contract on the use of Pageseal when the Controller installs Pageseal and applies from that time. It is concluded in electronic form (Article 28(9) GDPR) and needs no signature. Pageseal records the time of installation and the version of this agreement for the Controller’s store.

2. Nature, purpose, data and data subjects

- **Purpose:** creating and delivering personalised eBook copies, enforcing download limits, blocking links after cancellation or refund, tracing shared copies on the Controller’s request.
- **Data subjects:** the Controller’s buyers; the Controller’s staff who use Pageseal.
- **Data of buyers:** name, email address, Shopify customer ID, order ID and order number, checkout confirmation number, language; a random invisible code and a download link per copy; delivery status; download history (time, keyed hash of the IP address, shortened browser user agent, counter).
- **Data of staff:** the Shopify staff user ID in the log of access to buyer data.
- **Processing:** receiving order data from Shopify, storing it, writing name, order number and code into the copy, sending the delivery email, fulfilling the eBook order line in Shopify, deleting.

No special categories of personal data (Article 9 GDPR) are processed. The Service uses no artificial intelligence and makes no automated decisions about buyers.

3. Instructions

3.1 The Processor processes the data only on documented instructions of the Controller. The settings the Controller makes in Pageseal and this agreement are the instructions. This includes transfers to third countries, unless Union or Member State law requires otherwise; the Processor then informs the Controller beforehand, unless that law forbids it.

3.2 The Processor informs the Controller without delay if it considers an instruction to infringe data protection law.

3.3 The Controller is responsible for the lawfulness of the processing and for informing its buyers.

4. Confidentiality

Everyone at the Processor who has access to the data is bound to confidentiality or under a statutory obligation of confidentiality.

5. Security (Article 32 GDPR)

The Processor takes the technical and organisational measures in Annex 1 and may replace them with measures of at least the same level of protection.

6. Sub-processors

6.1 The Controller authorises the sub-processors in Annex 2.

6.2 The Processor informs the Controller by email to the store's contact address at least 30 days before adding or replacing a sub-processor. The Controller may object within that period for reasons of data protection; if no solution is found, the Controller may uninstall Pageseal.

6.3 The Processor imposes the same data protection obligations on each sub-processor by written contract and remains liable to the Controller for them.

7. Assistance

7.1 The Processor helps the Controller answer requests of data subjects (Articles 15 to 22 GDPR). Shopify's customers/data_request and customers/redact webhooks are handled automatically: the data stored about a buyer is sent to the Controller's contact email, and erasure is carried out as described in the Pageseal privacy policy.

7.2 The Processor helps the Controller with security, breach notification, data protection impact assessments and prior consultation (Articles 32 to 36 GDPR), taking into account the information available to it.

8. Personal data breaches

The Processor notifies the Controller without undue delay, and at the latest within 72 hours, after becoming aware of a personal data breach affecting the Controller's data, with the information available at that time, and supplements it as it becomes available.

9. Deletion and return

9.1 At the end of the processing the Controller chooses between return and deletion. For a return, the Controller asks the Processor by email before uninstalling and receives the buyer data stored for its store in a machine-readable format (JSON). Before uninstalling, the Controller can also view the delivery list in Pageseal.

9.2 After uninstallation the Processor deletes all of the Controller's data and files when Shopify sends the shop/redact webhook (48 hours after uninstallation), unless Union or Member State law requires storage. Only a SHA-256 hash of the store domain and the number of one-time free copies used are kept, so they are not granted again on reinstall. Personalised copies already downloaded by buyers are not affected.

10. Proof and audits

The Processor makes available all information necessary to demonstrate compliance with Article 28 GDPR and allows audits by the Controller or an auditor it mandates, after reasonable notice, during business hours and without access to other customers' data. The Controller bears its own costs.

11. US state privacy laws (CCPA)

11.1 Where the California Consumer Privacy Act as amended by the California Privacy Rights Act (Cal. Civ. Code § 1798.100 et seq., "CCPA") or a comparable US state privacy law applies, the Controller is the "business" and the Processor its "service provider" (Cal. Civ. Code § 1798.140(ag)). The Controller discloses personal information to the Processor only for the limited and specified business purposes in section 2.

11.2 The Processor does not: (a) sell or share the personal information; (b) retain, use or disclose it for any purpose other than the business purposes in this agreement, including any other commercial purpose; (c) retain, use or disclose it outside the direct business relationship with the Controller; (d) combine it with personal information it receives from or on behalf of another person, or collects from its own interaction with the consumer, except as the CCPA permits for service providers.

11.3 The Processor complies with the obligations of the CCPA that apply to it, provides the same level of privacy protection as the CCPA requires, and notifies the Controller if it determines that it can no longer meet these obligations. The Controller may take reasonable and appropriate steps to ensure that the Processor uses the personal information in line with the Controller's CCPA obligations (section 10), and, upon notice, to stop and remediate unauthorised use.

11.4 Sub-processors are engaged under section 6 and bound by written contract to the same requirements. Deletion requests of consumers reach the Processor through Shopify's customers/redact webhook and are carried out under section 7.1.

12. Final provisions

12.1 Where this agreement conflicts with other terms between the parties, this agreement prevails for data protection.

12.2 The Processor may update this agreement where the law or the Service changes. It informs the Controller by email to the store's contact address at least 30 days before the update applies. The update applies if the Controller keeps using Pageseal after that date; if the Controller does not agree, it may object in text form or uninstall Pageseal before that date.

12.3 German law applies. Place of jurisdiction is Hamburg, as far as legally permitted.

12.4 Other changes and side agreements must be in text form.

Annex 1 – Technical and organisational measures

- **Encryption in transit:** HTTPS for all connections to Pageseal; delivery emails are handed to Amazon SES over TLS.
- **Encryption at rest:** buyer name, email address and checkout confirmation number are encrypted field by field (Fernet: AES-128-CBC with HMAC-SHA256); exact matches use keyed hashes (HMAC-SHA256). Shopify access tokens and exports for data subject requests are encrypted as well. The keys are kept in a password vault and reach the application only as environment variables. Personalised eBook files contain the buyer's name by design; they are kept only as described under "Deletion".
- **Separation:** a separate database and folder per store; every request is bound to the store from the verified Shopify session token or webhook signature.
- **Authentication:** Shopify session tokens in the admin; webhooks verified with HMAC; download links random and limited in number and time.
- **Pseudonymisation:** IP addresses of downloads are stored only as a keyed hash; the invisible code is random.

- **Access control:** server access only for staff of the Processor who run the Service, with SSH keys (password login disabled) and a firewall. Every access to buyer data in the app (delivery list, leak search, re-sending the delivery email, data export, erasure) is logged with time, store, action, number of records and the acting user, without the data itself; the log is kept 12 months.
- **Incidents:** written incident procedure; the Controller is notified without undue delay, at the latest within 72 hours (section 8).
- **Availability:** hosting in a Hetzner data centre in Nuremberg, Germany; daily backups of the whole server by Hetzner in Germany, 7 versions kept.
- **Deletion:** automatic deletion on customers/redact and shop/redact; a daily job deletes download history and the access log after 12 months, personalised eBook files when their link is blocked or expired or after 30 days without a download, and exports for data subject requests after 30 days.
- **Test data:** development and tests use separate stores, keys and synthetic data, never production data.
- **Data minimisation:** no address, no phone number, no payment data; no artificial intelligence, no tracking.

Annex 2 – Sub-processors

Sub-processor	Service	Location and transfer basis
Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Germany	Hosting of the server, databases, files and backups	Data centre Nuremberg, Germany
Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855 Luxembourg	Sending delivery emails (Amazon SES)	EU region Stockholm (eu-north-1), Sweden; US parent company: EU-U.S. Data Privacy Framework, alternatively EU Standard Contractual Clauses
Cloudflare, Inc. 101 Townsend St, San Francisco, CA 94107, USA	Network in front of the app's web address (HTTPS, protection against attacks); requests to Pageseal, including buyers' downloads and IP addresses, pass through it	Cloudflare network, data centre nearest to the user; EU-U.S. Data Privacy Framework, alternatively EU Standard Contractual Clauses

Shopify is the Controller's own platform and not a sub-processor of Pageseal.