LEGAL

Data Processing Agreement

Version 1.0 · Last updated [DATE OF PUBLICATION]

This Data Processing Agreement ("**DPA**") forms part of the agreement between **Vrandex Media, obrt za usluge**, Ulica Velimira Terzića 13, 21000 Split, Croatia, OIB [OIB] ("**Processor**" or "**Vrandex**") and the customer that accepts the Vrandex Studio Terms of Service ("**Controller**" or "**Customer**"). It applies automatically when the Customer accepts the Terms. A signed copy is available on request at privacy@vrandexstudio.com.

Where the Customer is itself a processor (for example an agency acting for Client Brands), the Customer warrants that its controller has authorised it to engage Vrandex, and Vrandex acts as the Customer's sub-processor.

---

1. Definitions

Terms such as "personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "supervisory authority" have the meaning given in the **General Data Protection Regulation (EU) 2016/679** ("**GDPR**"). "**Customer Personal Data**" means personal data the Processor processes on behalf of the Controller when providing the Service, described in Annex I. "**Sub-processor**" means a third party engaged by the Processor to process Customer Personal Data.

2. Scope and roles

2.1 The Processor processes Customer Personal Data as processor on behalf of the Controller, only to provide the Service under the Terms.

2.2 The Processor is a separate controller for: account, billing and support data; security logs; usage data; and de-identified design data under section 9 of the Terms. That processing is governed by the Privacy Policy, not this DPA.

2.3 The Controller is responsible for the lawfulness of the processing it instructs, including having a legal basis for sharing Customer Personal Data with the Processor and providing the required notices to data subjects.

3. Instructions

3.1 The Processor processes Customer Personal Data **only on documented instructions** from the Controller, including for transfers to third countries, unless required by EU or Member State law; in that case, the Processor informs the Controller of that legal requirement before processing, unless the law prohibits it.

3.2 The Terms, this DPA, the Controller's configuration of the Service (including connecting Connected Services and choosing AI Features), and its approved actions in the Service are the Controller's complete documented instructions. Further instructions must be in writing and consistent with the Terms.

3.3 The Processor informs the Controller immediately if, in its opinion, an instruction infringes the GDPR or other data protection law.

4. Confidentiality

The Processor ensures that persons authorised to process Customer Personal Data are bound by confidentiality obligations or are under an appropriate statutory obligation of confidentiality, and access it only as needed for the Service.

5. Security

5.1 The Processor implements the technical and organisational measures in **Annex II**, appropriate to the risk, as required by Art. 32 GDPR.

5.2 The Processor may update the measures provided the overall level of security is not reduced.

6. Sub-processors

6.1 The Controller gives **general authorisation** for the Processor to engage the Sub-processors listed on the Sub-processors page (Annex III).

6.2 The Processor gives at least **30 days' notice** of any intended addition or replacement of a Sub-processor, by email to subscribers of the Sub-processors page and to the Workspace owner. The Controller may object on reasonable data-protection grounds within that period. The parties will discuss the objection in good faith; if no solution is found, the Controller may terminate the affected Service and receive a pro-rata refund of prepaid fees. In an emergency (for example to keep the Service secure or available), the Processor may replace a Sub-processor with shorter notice and will inform the Controller as soon as possible.

6.3 The Processor imposes on each Sub-processor, by contract, data protection obligations that provide at least the same level of protection as this DPA, and remains fully responsible to the Controller for its Sub-processors' performance.

6.4 Connected Services the Controller chooses (for example Shopify, WooCommerce, Klaviyo, Mailchimp, Vrandex Send) are not Sub-processors of the Processor; the Controller instructs the Processor to exchange data with them, and their own terms govern their processing.

7. International transfers

7.1 The Processor transfers Customer Personal Data outside the European Economic Area only where an adequate level of protection is ensured: by an adequacy decision (including the EU-US Data Privacy

Framework for certified recipients), or by the **Standard Contractual Clauses** adopted by Commission Implementing Decision (EU) 2021/914 (Module Three, processor to processor, between the Processor and the Sub-processor), with supplementary measures where needed.

7.2 To the extent the Controller is established outside the EEA and the Processor transfers Customer Personal Data back to it, Module Four of the Standard Contractual Clauses applies where required.

8. Assistance

8.1 **Data subject requests.** The Processor assists the Controller, by appropriate technical and organisational measures and as far as possible, in responding to requests from data subjects. If a data subject contacts the Processor directly about Customer Personal Data, the Processor forwards the request to the Controller without undue delay and does not answer it except on the Controller's instruction.

8.2 **Other assistance.** Taking into account the nature of the processing and the information available, the Processor assists the Controller with security (Art. 32), breach notification (Arts. 33–34), data protection impact assessments and prior consultation (Arts. 35–36). The Processor may charge reasonable costs for extensive assistance not caused by its own breach.

9. Personal data breaches

9.1 The Processor notifies the Controller **without undue delay and in any case within 48 hours** after becoming aware of a personal data breach affecting Customer Personal Data.

9.2 The notice includes, as far as available: the nature of the breach, categories and approximate number of data subjects and records, likely consequences, measures taken or proposed, and a contact point. Information may be provided in phases.

9.3 The Processor takes reasonable steps to contain the breach and mitigate its effects, and documents it.

9.4 Notification is not an acknowledgment of fault.

10. Deletion and return

10.1 After the end of the Service, the Controller can export its data for **30 days** as described in the Terms. After that, the Processor **deletes** Customer Personal Data within a further **30 days**, including copies, unless EU or Member State law requires storage. Data in backups is deleted when the backups rotate (at most **35 days** later) and is not restored in the meantime except to restore the Service.

10.2 For Shopify stores, shop data is deleted within 30 days after uninstall, as required by Shopify.

10.3 On request, the Processor confirms deletion in writing.

11. Audits and information

11.1 The Processor makes available to the Controller all information necessary to demonstrate compliance with Art. 28 GDPR, primarily through: this DPA, Annex II, the Sub-processors page, written answers to reasonable security questionnaires (once per year), and any certifications or reports the Processor holds.

11.2 If that information is not sufficient, the Controller may conduct an audit, by itself or through an independent auditor bound by confidentiality, at most **once per year** (or more often if required by a supervisory authority or after a breach), with at least **30 days'** written notice, during business hours, without access to other customers' data, and at the Controller's cost.

12. Liability

Each party's liability under this DPA is subject to the limitations in the Terms, except to the extent that GDPR Art. 82 provides otherwise for liability towards data subjects.

13. Term and precedence

This DPA lasts as long as the Processor processes Customer Personal Data. If this DPA conflicts with the Terms on data protection, this DPA prevails. If it conflicts with the Standard Contractual Clauses, the Standard Contractual Clauses prevail.

14. Governing law

This DPA is governed by the laws of the Republic of Croatia. The courts in Split, Croatia have jurisdiction, without prejudice to data subjects' rights under the GDPR.

Annex I: Description of the processing

Controller: the Customer (and, for agencies, its clients). Contact: the Workspace owner's email.

Processor: Vrandex Media, obrt za usluge, Split, Croatia, privacy@vrandexstudio.com.

Subject matter and nature: hosting, storage, analysis, generation and transmission of data to provide Vrandex Studio: designing marketing emails, generating texts and images with AI, planning campaigns, reading store and email-platform data, and pushing designs to the Customer's email platforms.

Purpose: providing the Service to the Customer as instructed.

Duration: for the term of the Agreement plus the deletion periods in section 10.

Categories of data subjects:

- the Customer's staff and contractors who use the Service (Authorised Users);
- people named or shown in the Customer's content (staff, models, influencers, customers quoted in reviews);
- the Customer's shoppers, **only** to the extent their data appears in store orders read to calculate product sales totals, or in reviews the Customer uploads;
- contacts in the Customer's email platforms, **only** as counts and campaign statistics (no individual contact data is stored by Vrandex Studio).

Categories of personal data:

- Authorised Users: name, email, role, profile picture, activity in the Workspace;
- content: names, images of people, quotes in reviews, any personal data the Customer chooses to include in briefs, emails or assets;
- store orders: order identifiers, line items, quantities, prices, discounts, refunds, dates and customer identifiers present in the order records, **processed transiently to calculate aggregated sales per product; names, email addresses, phone numbers and postal addresses are not stored**;
- email platforms: account identifiers, list and segment names, aggregated campaign statistics.

Special categories of data: not intended. The Customer must not upload special categories of personal data or data of children.

Frequency: continuous while the Service is used.

Retention: as in section 10 and the Privacy Policy.

Sub-processor processing: as in Annex III.

Annex II: Technical and organisational measures

1. **Encryption:** TLS 1.2+ for all data in transit; encryption at rest for databases and file storage (provider-managed AES-256); connection tokens for stores and email platforms encrypted with application-level keys; secrets stored in the hosting provider's encrypted environment, never in source code.
2. **Access control:** individual accounts only; multi-factor authentication on all administrative accounts (hosting, database, source code, auth provider, email, payments); least-privilege access; support access to customer Workspaces is view-only and logged; prompt removal of access when no longer needed.
3. **Application security:** workspace isolation enforced in every database query and tested automatically; input validation; protection against common web attacks; rate limits; signed webhooks verified (HMAC), with invalid signatures rejected; dependency updates and vulnerability alerts; security review before major releases.
4. **Logging and monitoring:** application and security logs; audit log of administrative and support actions; alerts on errors and abuse; log retention up to 365 days.

5. **Availability and resilience:** managed hosting and database with automatic backups and point-in-time recovery; restore tested periodically.
6. **Data minimisation:** read-only scopes for store connections; no storage of shoppers' names, emails, phone numbers or addresses; only aggregated sales stored; images sent to AI providers only when a feature needs them.
7. **Outbound control:** calls to Shopify's Admin API leave through a dedicated static-IP proxy that only allows connections to Shopify, with authentication.
8. **AI providers:** paid/commercial API tiers only; providers that do not train on API inputs are preferred; providers that do are disclosed (Annex III).
9. **Incident management:** documented breach response procedure; notification timelines as in section 9; post-incident review.
10. **Vendor management:** due diligence and data processing terms with every Sub-processor; transfer safeguards for non-EEA providers.
11. **People:** confidentiality obligations for everyone with access; security awareness.
12. **Deletion:** documented deletion on termination, Shopify uninstall and data-subject requests; backups expire within 35 days.

Annex III: Sub-processors

The current list of Sub-processors, with their location, purpose and transfer safeguard, is published at **vrandexstudio.com/subprocessors** and forms part of this DPA.

Vrandex Studio is a brand of Vrandex Media, obrt za usluge · Ulica Velimira Terzića 13, 21000 Split, Croatia · OIB [OIB] · support@vrandexstudio.com

© 2026 Vrandex Media, obrt za usluge