

# Rug Data Processing Addendum

Version 2026-10-02.1

## 1 Application and roles

This Rug Data Processing Addendum, version 2026-10-02.1 (DPA), forms part of the signed Rug Subscription Order Form and Rug Subscription Terms between Vizbl Systems, Inc. (Vizbl) and Customer. It applies to personal data Vizbl processes on Customer's behalf for the ordered rug services (Customer Personal Data). Customer acts as controller or business; Vizbl acts as processor, service provider or contractor as applicable. Customer acting as a processor for another controller requires a separately documented processing chain before use.

Applicable Data Protection Law means privacy and data-protection law applicable to the processing, including relevant US state laws and, where applicable, the GDPR, UK GDPR and Swiss FADP. Legal terms take their meaning from that law. A Security Incident means a breach of security causing accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

## 2 Processing instructions and limitations

Customer instructs Vizbl to perform only the processing described in Schedule A, this agreement and lawful documented instructions. Vizbl will promptly inform Customer if an instruction appears unlawful and pause the affected processing while the parties resolve it. If law requires other processing, Vizbl informs Customer beforehand unless prohibited. Customer is responsible for lawful collection, appropriate notices, necessary consents or other legal basis, and authorization to give instructions.

Vizbl will not sell Customer Personal Data, share it for cross-context behavioral advertising, use it for unrelated advertising, or retain, use or disclose it outside the direct business relationship or the specified purposes, except as expressly permitted by applicable law. It will not combine it with unrelated-source personal data except as legally permitted to provide the specified services. Customer materials, room photographs and derived visualizations are not used to train general-purpose or third-party AI models under this DPA.

Vizbl will provide the level of protection required by applicable law, comply with applicable processor and service-provider duties, and notify Customer if it can no longer meet them. Customer may take reasonable and appropriate steps to verify compliant use and stop and remedy unauthorized use. Vizbl certifies that it understands and will comply with these restrictions. Customer's service instructions do not authorize unrelated product development using identifiable shopper data.

## 3 Personnel and subprocessors

Vizbl restricts access to authorized persons bound to confidentiality and needing the data for their duties. Customer generally authorizes the subprocessors in the list made available before signature. The list must identify each provider's legal name, processing purpose and processing countries.

Vizbl contracts for materially equivalent protection, assesses suitability and remains responsible for subprocessor performance of these obligations.

Vizbl gives at least 30 calendar days' advance notice of a new or replacement subprocessor. Customer may object within that period on reasonable documented privacy grounds. Vizbl will work to resolve the concern or provide a reasonable alternative. If unresolved, either party may terminate the affected service before the new provider processes its data, without future affected fees and with a refund of unused prepaid affected fees. No provider may receive affected data before the required notice and objection process is complete.

## **4 Security and incidents**

Vizbl implements the safeguards in Schedule B and may improve them without materially reducing protection. Vizbl notifies Customer without undue delay and in any event within 48 hours after becoming aware of a Security Incident. It does not wait for a final forensic report. Notice includes available details of the incident, affected categories and approximate volumes, likely consequences, response measures and a contact, with material updates as investigation proceeds. Notice is not an admission of liability.

Vizbl contains, investigates and remedies the incident and reasonably assists Customer with legally required assessments and notices. Customer determines its own notification obligations; Vizbl may make any notification legally required of it. The parties coordinate where permitted. Contractual notice timing does not extend any statutory deadline.

## **5 Assistance and verification**

Vizbl reasonably assists Customer with access, correction, deletion, portability, restriction and objection requests, and with security duties, impact assessments and regulator consultations, taking account of the processing and information available. Vizbl forwards requests concerning Customer Personal Data to Customer promptly and does not respond substantively without instructions unless law requires. Customer authenticates requesters and sets the lawful response.

Vizbl supplies information needed to demonstrate compliance and permits proportionate audits by Customer or an independent confidential auditor. Existing reports and remote review may be used where sufficient. Ordinarily audits occur once yearly on 30 days' notice during business hours; shorter notice or additional audits are permitted for a material incident, credible noncompliance or legal or regulatory requirement. Security and confidentiality arrangements must not prevent legally required verification or regulator access.

Standard assistance is included. Extraordinary assistance may be charged only after prior agreement on reasonable cost, except where caused by Vizbl's breach, and payment negotiation must not delay compliance with a mandatory deadline. Other customers' data must remain protected during any review.

## 6 Retention and deletion

Customer may direct lawful earlier deletion. During active service, room photographs and their shopper-specific generated scenes are deleted from active systems within 30 days after upload; a shorter configured period applies when offered. The service does not include long-term saved shopper scenes unless the parties expressly agree on a different documented purpose and retention. Room photographs must not be copied into application logs or routine catalog exports.

Within 30 days after termination, Vizbl returns Customer Personal Data that remains lawfully available at Customer's choice, or deletes it, then deletes remaining active copies. The catalog export process does not extend photo retention. Protected backups are isolated from routine processing and deleted within 90 days after active deletion. If restored for disaster recovery, deletion instructions are reapplied. Vizbl confirms deletion on reasonable request.

Retention required by law is limited to the necessary data and period, with restricted access and continued protection; Vizbl informs Customer unless prohibited. Contract, billing and signature evidence that Vizbl lawfully retains for its own business and legal obligations is independent-controller data, not permission to retain shopper photographs or reuse Customer Personal Data.

## 7 International processing

Vizbl must disclose processing locations in the subprocessor list before processing. Where a restricted international transfer requires safeguards, the parties must establish and document a lawful transfer mechanism before that transfer. If EU standard contractual clauses are required, the applicable official clauses and completed annexes must be executed, together with any required UK or Swiss provisions and transfer assessment. This DPA alone does not constitute completed transfer clauses or assert participation in any certification or adequacy program.

Affected processing must not begin until required transfer documentation and safeguards are in place. This restriction also applies where a US Customer serves individuals whose data is subject to applicable international transfer requirements; Customer's incorporation country alone does not resolve the issue.

## 8 Relationship to the agreement

This DPA controls personal-data processing conflicts. Mandatory transfer clauses prevail for their applicable transfer. The liability provisions in Section 8 of the Rug Subscription Terms apply without creating a separate additional cap or limiting non-waivable individual or regulator rights. Accepted DPA versions cannot be changed by posting new text online; changes require mutual written acceptance, with any mandatory legal requirements applying directly.

Privacy notices go to the Customer notice contact in the Order Form and [legal@vizbl.com](mailto:legal@vizbl.com) for Vizbl. Customer may designate a separate security contact. Vizbl's own account, billing, contracting and legal-compliance processing is described in its Privacy Policy. This does not reclassify shopper photos or Customer-directed service processing as Vizbl's independent-controller activity.

## Schedule A Processing details

Subject matter: operating the rug visualization service selected in the Order Form. Duration: the service term plus the specific return, deletion and isolated-backup periods in Section 6. Frequency: on shopper or Customer request and routine support, security and retention operations.

Purposes and operations: receive product inputs and room photos; store and transmit them securely; render and return visualizations; manage the catalog and widget; provide Customer-facing service analytics; investigate faults and abuse; respond to authorized requests; and export or delete data. These are the limited business purposes for any applicable service-provider contract.

Individuals: Customer personnel and contractors using the service, shoppers and website visitors interacting with the widget, and persons incidentally depicted in voluntarily supplied photos. Data: relevant contact and account details, uploaded images and visualizations, IP addresses, browser/device details, interaction timestamps, support records and limited usage/security logs. Product-only images and data may be non-personal; this DPA applies only to their personal-data elements.

Prohibited inputs: intentionally submitted government identifiers, payment-card data, health records, biometric-identification data, intimate content, or other highly sensitive information unrelated to rug visualization. Customer must not target the service to children or invite uploads of people. The upload interface must tell shoppers to avoid photos showing people, documents or sensitive details. Incidental personal information remains protected by this DPA.

Retention: room photos and associated shopper-specific scenes, no more than 30 days in active systems after upload; operational usage/security logs, no more than 90 days unless a documented incident or legal requirement justifies restricted longer retention; Customer account and catalog personal data, during service and up to 30 days for return/deletion. Backup deletion follows Section 6. Subprocessors may not retain data longer than the applicable authorized period.

## Schedule B Security commitments

Access: unique identities, role-based least privilege, multi-factor authentication for privileged access, prompt access revocation, periodic access reviews, and confidentiality obligations. Support access to room photos is limited to a documented support or security need and is logged.

Data handling: encryption in transit using current TLS and encryption at rest for stored Customer Personal Data, secure key and secret management, segregation of customer records, private photo storage, short-lived authorized access links, data minimization and enforced retention/deletion jobs. Public catalog assets and private room photos have separate access rules.

Operations: security and access logging without raw photos or secrets; monitoring and incident-response procedures; risk-based vulnerability remediation; tested backup and recovery procedures; access-protected backups; secure change review; and controls to prevent accidental disclosure through logs, analytics, exports or development environments.

Providers: documented vendor review, written processing and confidentiality restrictions, a maintained subprocessor/location register, and controls disabling provider training or secondary use

of Customer images. Third-party model providers must have terms and configurations compatible with this DPA before receiving images.

These are contractual safeguards for the ordered service, not a statement of ISO, SOC or other certification and not a numerical uptime guarantee. Vizbl must maintain evidence that the safeguards are implemented throughout processing.