STYLDOD, INC.

Data Classification Matrix

Enterprise Policy Document

Document ID	DCM-001
Version	v1.0
Effective Date	June 2026
Document Owner	Senior Leadership / Engineering Leadership
Applies To	Enterprise embedded integrations, customer data, production systems, and all authorized personnel

Purpose

This Data Classification Matrix defines typical categories of data processed in Styldod enterprise embedded integrations and the intended handling approach. Customer-specific classifications may be agreed in the commercial agreement, DPA, or Statement of Work.

Data Classification Matrix

Data Category / Examples	Classification	Handling Approach
Selected input images (listing photo, room photo, exterior image, property image, optional reference image)	Customer Data / Potential Personal Data	Use only for agreed workflow. Restrict access. Protect in transit and at rest where supported.
User workflow inputs (text prompt, dropdown selection, style preference, room type, budget or product preference)	Customer Data / Potential Personal Data	Process only for service delivery and support. Avoid unnecessary collection.
Limited location data (zip code, postal code, city, or region for product discovery or localization where enabled)	Potential Personal Data	Use only for agreed functionality. Do not use for unrelated profiling or marketing.
Generated outputs (redesign, staging, editing, landscaping, exterior, or product visualization output)	Customer Data	Provide to customer workflow. Restrict access and retain according to agreement.
Workflow metadata (session ID, job ID, request ID, listing/photo reference, timestamp, processing status, error status)	Operational Customer Data	Used for support, troubleshooting, auditability, monitoring, and deletion requests.
Technical logs (CloudWatch/server logs, application logs, API logs, errors, performance and security events)	Operational/Security Data	Restricted access. Current standard log retention is generally 5 days unless otherwise agreed.
Direct identifiers (name, email, phone, payment data, government ID, platform credentials)	Not required by default for enterprise embedded workflow unless specifically agreed. If collected, treat as Personal Data with contractual controls.	Do not collect unless specifically agreed. Treat as Personal Data if present.

Sensitive/special category data (religious object in photo, person visible in photo, sensitive text typed by user)	Not intentionally collected. Incidental only.	Do not infer characteristics, identify individuals, or make decisions based on incidental sensitive data.
Customer internal business data (customer backend databases, internal business documents, confidential strategy/data)	Not required by default. If shared, treat as Confidential Customer Data.	Subject to agreement and need-to-know access only.

Handling Rules

- Use customer data only for agreed service delivery, support, monitoring, security, and contractual obligations.
- Do not use enterprise customer personal data for direct marketing unless expressly agreed.
- Do not use customer personal data or customer production data for unrelated public AI model training unless expressly agreed.
- Restrict access based on role, business need, and least privilege.
- Support customer deletion and data subject requests using workflow references where available.