STYLDOD, INC.

Data Subject Rights Request Procedure

Enterprise Policy Document

Document ID	DSR-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 and Scope

This procedure describes how Styldod supports enterprise customers in responding to data subject rights requests where relevant data is processed by Styldod and is under Styldod control. For enterprise embedded integrations, the customer generally acts as controller and is responsible for verifying identity, determining legal basis, and instructing Styldod where assistance is required.

Controller Verification Requirement

Styldod does not generally verify enterprise end-user identity directly because the embedded workflow may not require direct identifiers such as name, email, phone number, payment information, government ID, or customer platform credentials. The enterprise customer must verify the request and provide Styldod with documented instructions and sufficient search references.

Intake Requirements

When submitting a data subject rights request to Styldod, the enterprise customer must provide:

- Customer name and authorized requester/contact.
- Type of request: access, deletion, restriction, export, correction, objection, confirmation, or other.
- Session ID, job ID, request ID, listing/photo reference, timestamp, or workflow reference.
- Relevant environment or deployment (e.g. production, staging, customer-specific instance).
- Scope of request and any legal or contractual deadline.
- Whether legal hold, dispute, fraud/security, or preservation requirements apply.

Internal Search and Action Process

1. Log the request internally with date received, customer contact, request type, and target deadline.
2. Validate that the request came from an authorized customer contact or approved channel.
3. Identify likely systems containing relevant data (application database, cloud storage, workflow/job metadata, generated output storage, and logs).
4. Search using provided references such as session ID, job ID, request ID, listing/photo reference, or timestamp.
5. Assess available data and confirm whether the data is under Styldod control.
6. Perform the requested action where technically feasible and permitted by the agreement and applicable law.
7. Record actions taken, systems searched, data deleted/exported/restricted, exceptions, and completion date.
8. Respond to the customer through the agreed channel with confirmation or explanation of limitations.

Supported Actions

Request Type	Styldod Support
Access / Export	Locate relevant workflow data and provide available records or outputs to the enterprise customer, subject to agreement and technical feasibility.
Deletion	Delete relevant data under Styldod control from applicable production systems where feasible, subject to backups, legal holds, security needs, and contract terms.
Restriction	Restrict or suspend further processing of identified data where feasible and instructed by the customer.
Correction	Correct inaccurate operational metadata where feasible. Generated outputs or images may require deletion and regeneration rather than correction.
Objection	Support customer instructions to stop or limit processing where feasible and consistent with the service agreement.
Confirmation	Confirm whether identified workflow data exists under Styldod control, based on provided references.

Logs and Short-Retention Data

Current AWS CloudWatch/server logs are generally retained for 5 days and then automatically deleted. If a request relates to logs, the customer must provide relevant references promptly because logs may no longer be available after the configured retention period.

Exceptions and Limitations

- Styldod may be unable to locate data without sufficient session, job, request, listing, photo, or timestamp references.
- Data already deleted under retention schedules may not be recoverable.
- Backups may be deleted according to cloud-provider retention mechanisms and may not be immediately purgeable.
- Legal holds, security investigations, dispute requirements, or contractual obligations may limit immediate deletion.