

# Data Retention & Deletion Policy

*Procurement-friendly retention and deletion posture for security and procurement review (non-binding; contract may override).*

**Document ID:** MVG-RETENTION-1.0.2

**Version:** 1.0.2

**Effective date:** 2026-02-10

**Status:** Public

Formats: PDF (controlling) · DOCX (convenience)

**Classification:** Privacy / security policy addendum (B2B / procurement oriented)

**Contact:**

security@meridianverity.com (security)

## 1. Purpose

This policy describes MVG's retention and deletion posture for:

- website operational data (no-tracking-by-default posture),
- procurement, licensing, and evidence-request communications, and
- enterprise Services data processed under customer agreements (where applicable).

It is intended to reduce ambiguity during procurement and security review.

## 2. Order of precedence

- If you have a signed agreement with MVG, the agreement (and applicable DPA) controls retention and deletion for the Services.
- This policy provides default targets for contexts not governed by a signed agreement.
- Where law requires different retention (e.g., legal holds), law controls.

## 3. Retention principles

- Data minimization: collect and retain only what we need to operate securely and support legitimate business/procurement workflows.
- Purpose limitation: do not retain data longer than reasonably necessary for the purpose collected, unless legally required.
- Evidence-first safety posture: evidence artifacts are designed to minimize sensitive personal data and may use cryptographic commitments/pseudonymous identifiers.

## 4. Default retention targets (non-binding; may vary by context)

These are baseline targets for typical workflows. Actual periods may differ depending on security needs, incident investigation, or contractual requirements.

- Website access/security logs (IP, user-agent, request/response metadata): typically retained for a limited period for security and abuse prevention (often 30–180 days).
- Security vulnerability reports: retained for the life of the remediation record and audit trail (often 2–7 years depending on severity and regulatory posture).
- Procurement/licensing communications (emails, attachments you provide): retained as business records for a reasonable period (often up to 7 years), unless you request earlier deletion and we are not required to retain.
- Evidence request intake (via /trust/evidence): designed as a mailto-draft form (no site-side storage). Resulting email communications are treated as procurement communications above. If a

server-side intake is later introduced, submissions and minimal metadata are retained only as described here (typically aligned to the procurement communication period; logs retained 30–180 days).

- Evaluation materials received under NDA (non-public artifacts, claim sets, PoCs): retained only as permitted by the NDA/evaluation license and secured; deletion/return follows the agreement.
- Enterprise Services data (Customer Content, evidence artifacts, enforcement logs): retention is governed by the customer agreement and DPA; defaults may be configurable.
- Backups/archives: deletion follows backup cycles. Data in backups is protected and not used for new processing; it is deleted/overwritten according to standard backup retention unless legally required to retain.

## 5. Deletion and return

- Website context: you may request deletion of certain personal data we hold (subject to legal and security constraints).
- Enterprise context: at the end of Services, MVG will delete or return Customer Personal Data as provided in the DPA, subject to lawful retention requirements and backup cycles.
- Where feasible, MVG can provide written confirmation of deletion/return completion upon request.

## 6. Legal holds and mandatory retention

- MVG may retain data longer than the targets above where required to: comply with law or lawful government requests; establish, exercise, or defend legal claims; investigate and remediate security incidents; or preserve records subject to a legal hold.

## 7. Contact

- Privacy/DPA requests: [privacy@meridianverity.com](mailto:privacy@meridianverity.com)
- Procurement routing: [procurement@meridianverity.com](mailto:procurement@meridianverity.com)
- Security issues: [security@meridianverity.com](mailto:security@meridianverity.com)

## Change log

- v1.0.2 — Tightened language for public posting; standardized formatting; clarified PDF/DOCX roles.
- v1.0.1 — Added explicit treatment of /trust/evidence request intake and alignment guidance for any future server-side intake.
- v1.0.0 — Initial publication.