Data Retention and Deletion Policy

Dark Web Metrics — Retention Schedules, Deletion Procedures, Data Subject Rights

Dark Web Metrics — [LEGAL ENTITY]

May 2026 — Version 1.0

Contents

1 1. Purpose and scope

This policy defines how long Dark Web Metrics ("DWM", operated by [LEGAL ENTITY], a [JURISDICTION] limited liability company) retains the data it processes and how that data is deleted upon expiry, upon customer instruction, or upon a valid data subject request. It applies to every data category DWM holds, whether in primary storage, backup, log archive, or third-party sub-processor systems.

The policy is referenced by the Privacy Policy, the Data Processing Agreement, and the Information Security Whitepaper.

It is **not** an SLA. Maximum deletion timelines stated here are upper bounds; in many cases deletion occurs sooner.

2 2. Definitions

- **Customer Data.** Data the customer supplies to DWM (catalogs, configuration, account information).
- **Computed Data.** Indices and reports derived by DWM from external sources, scoped to the customer.
- **Signal Data.** Raw or normalized observations DWM has ingested from public or licensed sources, prior to scoping against any customer.
- **Operational Data.** Logs, metrics, internal telemetry, security event records.
- **Personal Data.** Information relating to an identified or identifiable natural person within the meaning of GDPR, UK GDPR, LGPD, APPI, CCPA/CPRA, and equivalent regimes.

3 3. Retention principles

DWM applies the following principles to every category:

1. **Purpose limitation.** Retain only as long as necessary for the documented purpose.
2. **Minimization.** Where retention is required, retain the minimum data needed for the purpose. Default to hashed or aggregated representations where the purpose allows.
3. **Determinable end.** Every retained item has a documented retention end-date, derivable either from its ingest timestamp or from a customer-specific configured horizon.
4. **Verifiability.** Deletion produces an internally auditable record. Customers may request a deletion attestation under their DPA.
5. **Legal holds preempt scheduled deletion.** Data subject to a valid legal hold (litigation, regulatory inquiry, internal investigation) is excluded from automated deletion until the hold is lifted, at which point default schedules resume.

4 4. Retention schedule

The following table is normative. Where a customer's contract specifies a shorter retention than the default, the contractual horizon prevails.

Category	Default retention	Storage location	Notes
Customer account record (active)	Life of account + 30 days	Supabase Postgres	Survives until cancellation

finalized. | | Customer billing record | 7 years from invoice issue | Supabase + Stripe + QuickBooks | Statutory; tax and accounting basis. | | Customer catalog (titles, fingerprints, performers, metadata) | 13 months rolling, configurable per tier up to 36 months | Supabase Postgres (Confidential) | Used for ongoing title matching. | | Customer brand and domain list | Life of account | Supabase Postgres | Required for scoping. | | Computed indices (PVS, TDI, SCE, PABMI, BIR) | 13 months default; 24 months Sentinel; 36 months Fortress | Supabase Postgres | Required to support trend reporting. | | Board deck PDFs | 36 months from generation | Supabase Storage | Audit and customer access. | | Evidence packages (signed) | 36 months from generation | Supabase Storage | Litigation support. | | Signal Data (torrent observations, forum mentions, etc.) | 13 months from observation | Supabase Postgres (Internal) | Pre-scoping; serves cross-tenant computation. | | Credential exposure — email hashes | 13 months from observation | Supabase Postgres | Sufficient to detect repeated leaks. | | Credential exposure — plaintext email (exceptional) | 30 days maximum | Encrypted bucket, restricted access | Retained only when needed for customer-side Art. 34 / §1798.82 notification. | | Plaintext password material | Never retained | — | Discarded at ingest after severity classification. | | Web session and audit logs | 12 months hot, 24 months cold | Better Stack | Security monitoring, incident investigation. | | Application error traces | 90 days | Sentry | Debugging. | | Backups (Postgres PITR) | 30 days rolling | Supabase | Disaster recovery. | | Sales/marketing contact data | 24 months from last interaction | HubSpot | Controller-mode. Subject to data subject requests. | | CSAM detection records (infohash + timestamp only) | Indefinite, minimal form | Encrypted log; access restricted | Reporting obligation to NCMEC or equivalent. No content retained. |

5 5. Deletion procedures

5.1 5.1 Routine deletion

A scheduled background job runs daily and deletes records whose retention end-date has passed, except for records under legal hold. The job produces an audit log entry per category indicating volume deleted.

5.2 5.2 Customer-initiated deletion (controller right)

A customer may request deletion of all or part of their Customer Data at any time via `privacy@darkwebmetrics.com` or through an authenticated mechanism in the dashboard. Deletion of all Customer Data and Computed Data scoped to that customer is completed within thirty (30) days of confirmed request, subject to:

- legal-hold exceptions (Section 3.5),
- retention of billing records as legally required (Section 4),
- retention of aggregated, anonymized data that cannot be re-associated to the customer.

A deletion attestation is provided to the customer upon completion.

5.3 5.3 Account termination

When a customer's account is terminated (for cause, non-renewal, or non-payment), DWM:

1. Disables access at 00:00 UTC on the termination date.
2. Provides a thirty (30) day export window during which the customer may retrieve their data.
3. At the end of the export window, executes deletion per Section 5.2 unless the customer has requested earlier deletion.

5.4 5.4 Data subject rights requests

DWM's role determines its responsibility:

- **DWM as processor (acting on a customer's behalf).** Requests received by DWM that pertain to a data subject whose personal data is held under a customer relationship are forwarded to the customer within five (5) business days for the customer to handle. DWM assists the customer to fulfil the request as required under the DPA.
- **DWM as controller (DWM's own marketing, sales, employee records).** Requests are handled directly by DWM. Acknowledgement within five (5) business days of receipt; substantive response within thirty (30) days, extendable by two months under GDPR Art. 12(3) where complexity justifies.

Rights handled include:

Regime	Rights handled
GDPR / UK GDPR	Articles 15 (access), 16 (rectification), 17 (erasure), 18 (restriction), 19 (notification), 20 (portability), 21 (objection), 22 (automated decision-making).
CCPA / CPRA	Right to know, right to delete, right to correct, right to opt-out of sale/sharing, right to limit use of sensitive personal information.
LGPD	Articles 17–22 (access, correction, anonymization, portability, deletion, information about sharing, etc.).
APPI	Disclosure, correction, addition or deletion, cessation of use, cessation of provision to third parties.
Other regimes	Handled by analogy and with counsel input where novel.

5.5 5.5 Sub-processor deletion

When customer data is deleted, DWM issues deletion instructions to relevant sub-processors per Section 6 of the DPA. Sub-processor deletion confirmations are recorded in the deletion audit log. Where a sub-processor's own retention obligations (e.g., Stripe's transaction records) exceed DWM's, the longer retention is disclosed.

5.6 5.6 Backup considerations

Customer data deletion is reflected in primary storage immediately upon execution of the deletion job. Backups containing the deleted data continue to exist until they age out of the backup retention window (Section 4). During that window, the deleted data is:

- not accessible through any production pathway,
- only restorable in the event of a full disaster-recovery scenario,
- subject to immediate re-deletion after any DR restoration that re-introduces it.

This approach is consistent with the European Data Protection Board guidance on backup-aware erasure.

5.7 5.7 Cryptographic deletion

For volumes encrypted with tenant-specific keys (where contractually required), deletion may be effected by destroying the relevant key material, rendering ciphertext unrecoverable. This option is available to Fortress-tier customers on request.

6 6. CSAM handling (special procedure)

CSAM is handled outside the general retention schedule due to its specific legal regime.

1. **Detection at ingest.** Heuristic classifiers and reference-hash matching identify suspected CSAM in incoming Signal Data.
2. **Immediate removal.** Content classified as CSAM is removed from indices and from raw storage within the same processing cycle.
3. **Minimal preservation.** Only the infohash (or equivalent content identifier) and detection timestamp are retained, and only in an encrypted log accessible to the Privacy Officer.
4. **Reporting.** Reports are filed with NCMEC (United States), the Internet Watch Foundation (United Kingdom), or other competent authorities as required by the applicable jurisdiction, in accordance with the CSAM Detection & Reporting Standard Operating Procedure.
5. **No further retention.** No copy of the underlying material is retained at any point.

7 7. Legal holds

A legal hold is initiated when DWM is on notice of pending or reasonably anticipated litigation, regulatory inquiry, or law-enforcement request. Holds are scoped to the minimum data necessary and are documented (initiator, scope, basis, expected end).

While a hold is in force, affected records are exempt from scheduled deletion. Customers whose data is on hold are informed where permitted by the applicable legal order.

8 8. Anonymization and aggregation

Aggregated and anonymized data (e.g., peer-cohort statistics in board decks) is retained beyond the underlying source data's retention period, on the basis that it is no longer Personal Data and no longer attributable to a specific customer. The anonymization process is documented in the Methodology Document, Section 11. DWM treats k-anonymity with $k \geq 5$ as the operational minimum and does not publish cohorts below that threshold.

9 9. Auditing and reporting

The retention and deletion processes generate:

- a daily deletion audit log (counts by category),
- a monthly internal review of retention compliance,
- a per-customer deletion attestation, on request,
- an annual external review (target: after first SOC 2 readiness assessment).

Customers may, under NDA and during business hours, request a sample of the deletion audit log relevant to their tenant.

10 10. Governance

The Privacy Officer owns this policy and reviews it at least annually and upon material change in applicable law, infrastructure, or service. Changes are version-controlled, communicated to customers in the regular sub-processor and policy-update channels, and reflected in the dated version footer.

11 11. Contact

- Privacy and DSAR requests: `privacy@darkwebmetrics.com`
- Customer deletion attestations: `privacy@darkwebmetrics.com`
- CSAM reports (external): see Information Security Whitepaper, Section 13.5.
- Legal: `legal@darkwebmetrics.com`

End of document. Data Retention and Deletion Policy version 1.0 — effective May 2026.