exposurebureau.com

exposure bureau

DIGITAL-RISK QUANTIFICATION

PUBLIC

Data Retention & Deletion Policy

Exposure Bureau — retention schedules, deletion procedures, data subject rights

DOCUMENT DOC 04 VERSION v2.0 DATE 2026-05-23 ENTITY Exposure Bureau LLC

This policy defines how long Exposure Bureau LLC ("Exposure Bureau", "the Company", a US 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 the Company holds, whether in primary storage, backup, log archive, or third-party subprocessor systems. The policy is referenced by the Privacy Policy, the Data Processing Agreement (DPA), and the Information Security Whitepaper. It is not an SLA: maximum deletion timelines stated here are upper bounds; in many cases deletion occurs sooner.

> COUNSEL REVIEW
>
> Confirm that the data-subject-rights enumeration (Section 5.4), the statutory billing-retention period (Section 4), legal-hold scope (Section 7), and the cross-border deletion-instruction flow to subprocessors (Section 5.5) match the executed DPA, Privacy Policy, and applicable regimes (GDPR/UK GDPR, CCPA/CPRA, LGPD, APPI). The 13-month default and per-category configurability must align with the MSA and DPA.

1 Purpose and scope

This policy governs retention and deletion of all data Exposure Bureau processes in delivering its recurring intelligence reports, one-shot diligence reports, and roadmap API access. The Company is report-first and does not operate a self-serve dashboard.

2 Definitions

- **Customer Data.** Data the customer supplies (brand and domain lists, configuration, account information).
- **Computed Data.** Indices and reports derived by the Company from external sources, scoped to the customer.
- **Signal Data.** Raw or normalized observations the Company 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 Retention principles

1. **Purpose limitation.** Retain only as long as necessary for the documented purpose.
2. **Minimization.** Retain the minimum data needed. Identifiers are hashed at ingest (`SHA-256` with a 90-day rotating per-tenant salt); the Company stores the hash plus observation metadata only. Default to hashed or aggregated representations where the purpose allows.
3. **Determinable end.** Every retained item has a documented retention end-date, derivable from its ingest timestamp or a customer-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 under a valid legal hold is excluded from automated deletion until the hold is lifted, at which point default schedules resume.

4 Retention schedule

The following table is normative. Where a customer's contract specifies a shorter retention than the default, the contractual horizon prevails. The default for collected signals and computed indices is **13 months**, configurable per category and per tier.

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 brand and domain list	Life of account	Supabase Postgres	Required for scoping queries.
Computed indices (`CES`, `IMI`, `RPS`, `BLV`, `BIR`, full family + composite `CXI`)	13 months default; configurable per tier up to 36 months	Supabase Postgres (Confidential)	Required to support trend reporting.
Recurring report and board-deck PDFs	36 months from generation	Supabase Storage	Audit and customer access.
Evidence packages (signed)	36 months from generation	Supabase Storage	Litigation and diligence support.
Signal Data (leak-site mentions, IAB listings, paste/forum observations)	13 months from observation	Supabase Postgres (Internal)	Pre-scoping; serves cross-tenant computation.
Credential exposure — identifier hashes (SHA-256 + 90-day rotating per-tenant salt)	13 months from observation	Supabase Postgres	Sufficient to detect repeated leaks; no plaintext stored.
Credential exposure — plaintext identifier (exceptional)	30 days maximum	Encrypted bucket, restricted access	Retained only on verified domain ownership + lawful basis, e.g. 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.

CATEGORY	DEFAULT RETENTION	STORAGE LOCATION	NOTES
Application error traces	90 days	Sentry	Debugging.
Backups (Postgres PITR)	30 days rolling	Supabase	Disaster recovery.
Sales/marketing contact data (first-party leads)	24 months from last interaction	HubSpot / Supabase	Controller-mode; consent basis. Subject to data subject requests and deletion path.

5 Deletion procedures

5.1 Routine deletion

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

5.2 Customer-initiated deletion (controller right)

A customer may request deletion of all or part of their Customer Data at any time via hello@exposurebureau.com or through an authenticated mechanism. 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),
- 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 upon completion. First-party leads (waitlist and resource requests) follow the same path: a deletion request resolves to the `delete_lead_by_email(text)` routine, which cascades to associated report subscriptions.

5.3 Account termination

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

5.4 Data subject rights requests

The Company's role determines its responsibility:

- **Exposure Bureau as processor** (acting on a customer's behalf). Requests pertaining 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. The Company assists as required under the DPA.

- **Exposure Bureau as controller** (the Company's own marketing, sales, employee records). Requests are handled directly. Acknowledgement within five (5) business days; substantive response within thirty (30) days, extendable by two months under GDPR Art. 12(3) where complexity justifies.

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, delete, correct, opt-out of sale/sharing, and limit use of sensitive personal information.
LGPD	Articles 17–22 (access, correction, anonymization, portability, deletion, information about sharing).
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 Subprocessor deletion

When customer data is deleted, the Company issues deletion instructions to relevant subprocessors per the DPA. Subprocessor deletion confirmations are recorded in the deletion audit log. Where a subprocessor's own retention obligations (e.g., Stripe's transaction records) exceed the Company's, the longer retention is disclosed.

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 a full disaster-recovery scenario,
- subject to immediate re-deletion after any DR restoration that re-introduces it.

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

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 top-tier customers on request.

6 CSAM handling (special procedure)

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

1. **Detection at ingest.** Reference-hash matching and classifiers identify suspected CSAM in incoming Signal Data.

2. **Immediate removal.** Content classified as CSAM is removed from indices and raw storage within the same processing cycle.
3. **Minimal preservation.** Only the content identifier (hash) and detection timestamp are retained, 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, per the CSAM Detection & Reporting Standard Operating Procedure.
5. **No further retention.** No copy of the underlying material is retained at any point.

7 Legal holds

A legal hold is initiated when the Company is on notice of pending or reasonably anticipated litigation, regulatory inquiry, or law-enforcement request. Holds are scoped to the minimum data necessary and 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 Anonymization and aggregation

Aggregated and anonymized data (e.g., peer-cohort statistics in reports) 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. The Company treats k-anonymity with $k \geq 5$ as the operational minimum and does not publish cohorts below that threshold.

9 Auditing and reporting

- 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 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 subprocessor and policy-update channels, and reflected in the dated version footer.

11 Contact

- Privacy and DSAR requests: hello@exposurebureau.com
- Customer deletion attestations: hello@exposurebureau.com
- CSAM reports (external): see Information Security Whitepaper.
- Legal: hello@exposurebureau.com

End of document. Data Retention & Deletion Policy version v2.0 — effective 2026-05-23. Exposure Bureau LLC, exposurebureau.com.