

Data Retention and Deletion Statement

Version 1.0 · June 2026

This statement summarises the retention and deletion practices applied by RADAR FORGE (the “Processor”) to personal data processed on behalf of the Controller under the LeakRadar Data Processing Agreement (DPA). For the full contractual framework, see DPA Sections 5 and 9, and Annexes 1 and 3.

1. Retention by data category

Data category	Retention period	Reference
Account data (name, business email, hashed credentials, role)	Active subscription + 90 days post-termination, then deleted or anonymised	DPA §9.1
Configuration data (monitored domains and assets)	Active subscription + 90 days post-termination	DPA §9.1
Support data (contact details, live-chat content, IP, connection metadata)	Active subscription + 90 days post-termination	DPA §9.1
Billing data (billing contact, company details, invoices, transactions)	10 years from issuance (French statutory accounting and tax obligations)	Art. L123-22 Code de commerce; CGI
Technical logs (access, application, system logs)	Up to 12 months from creation, then auto-purged	DPA Annex 3
Backups (encrypted production snapshots)	12 months rolling retention; oldest backups auto-pruned	Privacy Policy §4
Inactive accounts (no activity for 12 consecutive months)	Account and associated personal data deleted after 12 months of inactivity	Privacy Policy §4

2. Deletion at end of service

Upon termination of the Service, the Processor deletes or anonymises the Controller’s account, configuration and support data within ninety (90) days, save for data that must be retained to comply with a legal obligation (billing records, as set out above). Within the same ninety (90) day period, the Processor provides the Controller with a written certificate confirming that the deletion or anonymisation has been completed, identifying any data retained on legal grounds and the corresponding retention period.

Upon the Controller’s written request made before the end of that period, the Processor instead returns the personal data in a commonly used format and then deletes it.

3. Data subject rights — response times

The Processor assists the Controller in responding to requests from data subjects under Chapter III GDPR, within the statutory time frame of one (1) month from receipt of the request (Article 12(3) GDPR), extendable by two (2) further months where necessary, taking into account the complexity and number of requests.

This applies to: right of access (Art. 15), right to rectification (Art. 16), right to erasure (Art. 17), right to restriction (Art. 18), right to data portability (Art. 20), and right to object (Art. 21).

4. Backups

Production backups are encrypted at rest using AES-256 and retained on a twelve-month rolling basis. Backups containing data subject to deletion are overwritten in the normal rotation within the rolling window. The Processor does not selectively delete individual records from backup media; deletion is achieved through the rolling rotation cycle.

5. Periodic review

Retention periods and deletion practices are reviewed periodically and may be updated to reflect operational, legal or regulatory developments, provided the level of protection is not diminished.