Technical and Organisational Measures (TOMs)

Version 1.1 · June 2026

This document describes the technical and organisational security measures implemented by RADAR FORGE (the "Processor") in respect of personal data processed on behalf of the Controller under the LeakRadar Data Processing Agreement (DPA). It is aligned with the requirements of Article 32 of Regulation (EU) 2016/679 (GDPR) and is consistent with Annex 3 of the DPA, of which it forms an expanded presentation. In case of conflict, the DPA prevails.

1. Approach to security

The Processor implements measures appropriate to the nature, scope, context and purposes of the processing carried out for the Controller, and to the risks of varying likelihood and severity for the rights and freedoms of natural persons. Measures are reviewed periodically and may be updated to reflect technical and organisational developments, provided the level of security is not diminished.

2. Pseudonymisation and encryption (Art. 32(1)(a))

Encryption in transit. All connections to the Service, its API, and between infrastructure components are encrypted using TLS 1.3.

Encryption of backups at rest. All production backups are encrypted at rest using AES-256.

Password storage. User login passwords are stored as salted cryptographic hashes (bcrypt, cost 12). Plaintext passwords are never written to disk and are not retained.

At-rest protection of production storage (compensating controls). The Controller’s account and configuration data stored in the live production database are not subject to full-volume disk-level encryption at rest. The Processor has assessed the residual risk under Article 32 GDPR and applies the following compensating controls, which together are considered appropriate to that risk:

- EU/EEA-only hosting of production data, on dedicated bare-metal infrastructure operated under contract with Hetzner Online GmbH (Finland) and OVH SAS (France); no shared multi-tenant database.
- Physical and environmental security inherited from EU/EEA Tier-III/IV data centres operated by the hosting providers, with end-of-life secure media disposal procedures.
- Strict network segmentation; the production database is not exposed to the public internet and is reachable only from authorised application hosts within a private network.
- Role-based access control with the principle of least privilege; administrative access restricted to a limited number of authorised personnel.
- Multi-factor authentication (MFA) enforced on all administrative and infrastructure access.
- Login passwords stored only as salted bcrypt hashes; plaintext passwords are never written to disk.
- All backups encrypted at rest with AES-256.
- Centralised logging and monitoring of access to production systems, with alerting on anomalous activity; logs retained for up to 12 months.

3. Confidentiality, integrity, availability and resilience (Art. 32(1)(b))

Confidentiality. Access to personal data is restricted to authorised personnel on a need-to-know basis through role-based access control. Multi-factor authentication is enforced on all

administrative and infrastructure access. Network segmentation isolates the production environment.

Integrity. Centralised logging and monitoring detect anomalous activity. Production environments are logically isolated from development and testing environments. Changes to the production environment are deployed through a controlled pipeline (see Section 6).

Availability. Production workloads are hosted on dedicated infrastructure in EU/EEA Tier-III/IV data centres. Encrypted backups support availability and restoration of data.

Resilience. Production data is backed up regularly to encrypted off-cluster storage (12-month rolling retention, AES-256). Monitoring and alerting cover system events and application activity.

4. Ability to restore availability and access (Art. 32(1)(c))

Encrypted backups support the restoration of availability and access to personal data in the event of a physical or technical incident. Restoration is carried out on a best-effort basis. The Processor does not currently commit to specific Recovery Time Objective (RTO) or Recovery Point Objective (RPO) targets in the context of the Service, given its present operational scale and the absence of a 24/7 service level commitment.

5. Regular testing, assessing and evaluating effectiveness (Art. 32(1)(d))

The Processor monitors security advisories and vulnerability disclosures relevant to the components in use. Security-relevant patches are applied promptly upon assessment. Access rights are reviewed periodically. Technical and organisational measures are themselves reviewed periodically.

6. Specific controls

6.1 Access control and authentication

- Role-based access control restricting access to personal data to authorised personnel on a need-to-know basis.
- Multi-factor authentication (MFA) enforced on all administrative and infrastructure access (hosting consoles, source-code repositories, deployment tooling, email, payment processor, accounting).
- Strong cryptographic storage of user passwords (salted bcrypt, cost 12); plaintext passwords are not retained.
- Periodic review of access rights; removal of access on personnel changes.

6.2 Network and infrastructure security

- TLS 1.3 enforced for all external and inter-component connections.
- Production database not exposed to the public internet; reachable only from authorised application hosts within a private network.
- Edge protection (DDoS mitigation, WAF, DNS) provided by Cloudflare.
- Logical isolation between production, staging and development environments.
- Hosting on dedicated bare-metal infrastructure in EU/EEA data centres (Hetzner Online GmbH in Finland, OVH SAS in France).

6.3 Application security and change management

Application source code is managed in a version-controlled repository with access restricted to authorised personnel. Changes are deployed to production through a continuous integration /

continuous deployment (CI/CD) pipeline, with a separate staging environment used for pre-production validation. Dependency and supply-chain advisories are monitored.

6.4 Logging and monitoring

Centralised logging captures access events on production systems and application activity, with alerting on anomalous patterns. Logs are retained for up to 12 months and then auto-purged. Product analytics are processed via PostHog Cloud EU (Frankfurt, Germany). Audience and advertising analytics for the public website and the members application are processed via Google (Google Analytics 4 and Google Ads) under the EU-U.S. Data Privacy Framework; see the Sub-Processor List. Search query content is not logged; only operational metadata (timestamp, account identifier, search type, and internal leak identifier for purchased unlocks) is retained for billing reconciliation and abuse prevention, in accordance with Terms of Service section 3.

6.5 Vulnerability and patch management

The Processor maintains awareness of security advisories and CVE disclosures relevant to its technology stack. Security-relevant patches are reviewed and applied as part of regular operational maintenance, with prioritisation determined by assessed severity and exposure.

6.6 Backup and recovery

Production data is backed up to encrypted off-cluster storage within the EU/EEA. Backups use AES-256 encryption at rest and are retained on a twelve-month rolling basis. Restoration is performed on a best-effort basis as described in Section 4.

6.7 Physical security

Physical security of production infrastructure is inherited from the hosting providers' EU/EEA Tier-III/IV data centres (Hetzner Online GmbH, OVH SAS), which operate access control, environmental controls, fire suppression, redundant power and connectivity, and end-of-life secure media disposal procedures. The Processor does not operate its own physical premises housing production data.

7. Personnel and organisational measures

RADAR FORGE is a single-operator company. The President (Alexandre Vandamme) is the sole authorised personnel with access to production systems and to personal data processed on behalf of the Controller, and is bound by statutory confidentiality obligations as a corporate officer under French law. No employees, contractors or interns currently have such access.

The Processor uses Dougs, a French cloud-based accounting platform, for its own statutory accounting and tax obligations. Dougs has access only to the Processor's internal accounting records (including invoices issued to the Controller in the course of the commercial relationship); Dougs does not have access to Service infrastructure, monitored-asset configurations, or any personal data processed by the Service on behalf of the Controller.

Confidentiality commitments bind all personnel with access to personal data. Engagement of any sub-processor is conditioned upon contractual data-protection obligations equivalent to those in the DPA.

8. Sub-processor management

Sub-processors are engaged only under contractual data-protection obligations equivalent to those in the DPA (Section 6.3). The current list of sub-processors is maintained as a separate document and in Annex 2 of the DPA. Changes are notified to the Controller at least thirty (30) days in advance, giving the Controller the opportunity to object on reasonable data-protection grounds.

9. Incident response and breach notification

Detection. Incidents are detected via centralised logging, monitoring and alerting on anomalous activity.

Reporting channel for external researchers. A coordinated vulnerability disclosure channel is published at https://leakradar.io/.well-known/security.txt, with the contact address contact@leakradar.io.

Notification to the Controller. The Processor notifies the Controller of any personal data breach affecting the Controller's personal data without undue delay and in any event within twenty-four (24) hours of becoming aware of it. A substantive update including the information required under Article 33(3) GDPR is provided within forty-eight (48) hours of the initial notification, as set out in Section 8 of the DPA.

Cooperation. The Processor assists the Controller in meeting its own notification obligations to supervisory authorities (Art. 33) and to affected data subjects (Art. 34), taking into account the nature of processing and the information available to the Processor.

10. Periodic review

These TOMs are reviewed periodically and may be updated to reflect technical and organisational developments, provided the level of security is not diminished. Material changes affecting the Controller will be communicated in accordance with the DPA.