DATA PROCESSING AGREEMENT

Pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR)
Version 2.3 (final), June 2026

1. The Parties

This Data Processing Agreement (the "DPA") is entered into between:

The Processor
RADAR FORGE, a simplified joint-stock company (SASU) registered in France under SIREN 100187533, with a share capital of EUR 1,000, with its registered office at 60 rue François 1er, 75008 Paris, France, operating the service "LeakRadar" (leakradar.io), represented by Alexandre Vandamme, President (hereinafter "RADAR FORGE" or the "Processor").

The Controller
The customer entity subscribing to the LeakRadar service, identified as follows (to be completed by the Controller):

Legal entity name: _____

Company registration no.: _____

Registered address: _____

Represented by (name, title): _____

(hereinafter the "Controller").
The Processor and the Controller are individually referred to as a "Party" and collectively as the "Parties".

2. Background and Scope

2.1 The Controller has subscribed to the LeakRadar service (the "Service"), under which the Processor provides a credential-exposure monitoring and threat-intelligence platform.

2.2 In the course of providing the Service, the Processor processes personal data on behalf of the Controller, namely the Controller's account and usage data (e.g. user login credentials, monitored domains, billing information, and support communications). This DPA governs that processing.

2.3 Distinct controllership over indexed data. Separately from this DPA, RADAR FORGE acts as an independent data controller in respect of the compromised-credential datasets it indexes from publicly available breach and leak sources. This includes the surfacing of credential-exposure results matching a domain or asset, which RADAR FORGE performs on the basis of its own pre-existing datasets and legal basis, within the French CNIL framework applicable to the re-use of illegally leaked information ("RIFI"). That activity is carried out under RADAR FORGE's own controllership and does not fall within the scope of this DPA; the Controller has no controllership, instruction rights, or responsibility over those datasets.

2.4 In the event of any conflict between this DPA and the main service agreement or terms of service between the Parties (the "Main Agreement"), this DPA prevails with respect to the processing of personal data.

3. Definitions

Terms such as "personal data", "processing", "data subject", "controller", "processor", "sub-processor", and "personal data breach" have the meanings given to them in the GDPR.

"Applicable Data Protection Law" means the GDPR and any national legislation implementing or supplementing it, including the French Data Protection Act (Loi Informatique et Libertés).

4. Subject Matter and Duration of Processing

4.1 The subject matter, nature, purpose, duration of the processing, the types of personal data, and the categories of data subjects are described in Annex 1.

4.2 This DPA forms an integral part of the Main Agreement and governs all processing of personal data carried out by the Processor on behalf of the Controller. It is incorporated into the Main Agreement by reference and is binding without separate signature: it takes effect on the Controller's acceptance of the Main Agreement or first use of the Service, whichever is earlier, and remains in force for as long as the Processor processes personal data on behalf of the Controller under the Main Agreement. The Processor's signature is pre-applied to the published version of this DPA; the signature blocks in Section 11 are provided for Controllers that require a counter-signed copy, and where the Parties execute this DPA it also takes effect on the date of last signature.

5. Obligations of the Processor

The Processor shall:

- Process personal data only on documented instructions from the Controller, including with regard to transfers, unless required to do so by Union or Member State law; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless the law prohibits such information on important grounds of public interest. The Main Agreement, this DPA, and the Controller's configuration and use of the Service constitute the Controller's documented instructions.
- Ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in Annex 3, in accordance with Article 32 GDPR.
- Respect the conditions for engaging sub-processors set out in Section 6.
- Taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as possible, for the fulfilment of the Controller's obligation to respond to requests for exercising data subject rights under Chapter III GDPR.
- Assist the Controller in ensuring compliance with its obligations under Articles 32 to 36 GDPR (security, breach notification, data protection impact assessments, and prior consultation), taking into account the nature of processing and the information available to the Processor.
- At the choice of the Controller, delete or return all personal data after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data (see Section 9).
- Make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR, and allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, subject to Section 8.

The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Applicable Data Protection Law.

6. Sub-processors

6.1 The Controller grants the Processor general written authorisation to engage the sub-processors listed in Annex 2 for the performance of the Service.

6.2 The Processor shall inform the Controller of any intended changes concerning the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the

Controller the opportunity to object to such changes. If the Controller objects on reasonable data-protection grounds, the Parties shall discuss the objection in good faith. If, despite such discussions, the Parties cannot agree on an alternative within a reasonable period, the Controller may terminate the affected Service without penalty by giving written notice to the Processor, with a pro-rata refund of any prepaid fees corresponding to the unused portion of the subscription term.

6.3 Where the Processor engages a sub-processor, it shall do so by way of a contract imposing on the sub-processor data protection obligations substantially equivalent to those set out in this DPA. The Processor remains fully liable to the Controller for the performance of the sub-processor's obligations.

7. International Transfers

7.1 All customer account and monitoring data central to the Service is hosted within the European Union / European Economic Area (data centres located in France and Finland).

7.2 Certain sub-processors listed in Annex 2 are established outside the EEA or may process limited categories of personal data (e.g. email address, IP address, request metadata, or support-chat content) on infrastructure located outside the EEA. Where such processing involves a transfer of personal data outside the EEA, the Processor ensures that an appropriate transfer mechanism under Chapter V GDPR is in place, namely (i) an adequacy decision, including the EU-U.S. Data Privacy Framework where the sub-processor is certified, or (ii) the European Commission's Standard Contractual Clauses together with any supplementary measures required. Details of the mechanism applicable to each sub-processor are set out in Annex 2 and may be provided on request.

8. Personal Data Breach and Audit

8.1 The Processor shall notify 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. The initial notification shall contain the information then reasonably available. The Processor shall provide a substantive update with the further information required under Article 33(3) GDPR (nature of the breach, categories and approximate number of data subjects and records concerned, likely consequences, and measures taken or proposed) within forty-eight (48) hours of the initial notification, to enable the Controller to meet its own notification obligations under Articles 33 and 34 GDPR.

8.2 The Processor shall make available the information necessary to demonstrate compliance with this DPA. Audits may be conducted by the Controller or by an independent third-party auditor appointed by the Controller and bound by appropriate confidentiality obligations. Audits shall be conducted at the Controller's expense, upon reasonable prior written notice (at least thirty (30) days), no more than once per twelve-month period except following a personal data breach, during normal business hours, and in a manner that does not unreasonably disrupt the Processor's operations or compromise the confidentiality of other customers' data. The Processor may satisfy audit requests by providing existing documentation, security questionnaires, or third-party reports where available.

9. Return and Deletion of Data

9.1 Upon termination of the Service, the Processor shall delete or anonymise the Controller's account and monitoring personal data within ninety (90) days, save for data that must be retained to comply with a legal obligation (for example, billing records retained in accordance with applicable French accounting and tax law). The Processor shall, within the same period, provide 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.

9.2 Upon the Controller's written request made before the end of that period, the Processor shall instead return the personal data in a commonly used format and then delete it.

10. Liability and Miscellaneous

10.1 Notwithstanding any limitation of liability contained in the Main Agreement, each Party's aggregate liability arising out of or in connection with this DPA, whether in contract, tort (including negligence), breach of statutory duty or otherwise, is capped at an amount equal to ten (10) times the fees paid or payable by the Controller to the Processor under the Main Agreement during the twelve (12) months preceding the event giving rise to the claim. This cap shall not apply to liability that cannot be excluded or limited under applicable law, including liability arising from fraud, wilful misconduct or gross negligence (faute lourde ou dolosive) under French law.

10.2 Notices under this DPA, including notifications of personal data breaches, intended changes to sub-processors, and certificates of deletion, shall be delivered by email to the contact addresses designated by each Party. The Controller's notification email address shall be provided to the Processor and may be updated by written notice.

10.3 This DPA is governed by French law. Any dispute relating to it shall be subject to the jurisdiction of the competent courts of Paris, France, unless otherwise agreed in the Main Agreement.

10.4 If any provision of this DPA is held invalid or unenforceable, the remaining provisions remain in full force and effect.

11. Signatures

This DPA is binding on both Parties through its incorporation into the Main Agreement (Section 4.2). Signature below is optional and provided for Controllers that require a counter-signed copy. The Processor's signature is pre-applied to the published version.

For the Processor (RADAR FORGE)	**For the Controller**
Name: Alexandre Vandamme	Name: _____
Title: President	Title: _____
Date: _____	Date: _____
Signature: */s/ Alexandre Vandamme*	Signature: _____

Annex 1. Description of the Processing

Item	Description
Subject matter	Processing of the Controller's account and usage data necessary to provide the LeakRadar credential-exposure monitoring service.
Nature and purpose	Account creation and authentication; configuration and monitoring of the Controller's designated domains/assets; generation of exposure alerts and reports; billing; and customer support.
Duration	For the duration of the Main Agreement, followed by deletion or anonymisation in accordance with Section 9 (within 90 days of termination, subject to legal retention obligations).
Categories of data subjects	The Controller's authorised users and administrators of the Service.
Categories of personal data	Account data: name, business email, login credentials (hashed), role. Configuration data: monitored domains and assets. Billing data: billing contact, company details, transaction records. Support data: contact details and connection data (e.g. IP address) processed via the live-chat tool. Technical data: IP address, log and usage metadata.
Special categories	None are intentionally processed. The Service is not designed to process special categories of personal data under Article 9 GDPR.

Annex 2. Authorised Sub-processors

The following sub-processors are authorised to process the Controller's personal data in connection with the Service:

#	Sub-processor	Purpose	Location	Transfer mechanism
1	Hetzner Online GmbH	Hosting and infrastructure (data centre: Finland)	Germany / Finland	Intra-EU/EEA
2	OVH SAS	Hosting and infrastructure	France	Intra-EU/EEA
3	Stripe Payments Europe, Ltd.	Card payment processing	Ireland	Intra-EU/EEA
4	Railsware Products Studio LLC (Mailtrap)	Transactional email delivery	USA	EU-U.S. Data Privacy Framework
5	Zoho Corporation B.V. (Zoho Mail)	Business email hosting (contact@leakradar.io inbox)	Netherlands	Intra-EU/EEA; EU-U.S. DPF / SCCs for any US group-entity access
6	PostHog, Inc. (PostHog Cloud EU)	Product analytics	Germany / Frankfurt	Intra-EU/EEA
7	Google Ireland Limited / Google LLC (Google Analytics, Google Ads)	Audience analytics and advertising conversion measurement (public website and members application)	Ireland / USA	EU-U.S. Data Privacy Framework (Google LLC) / SCCs
8	tawk.to Inc.	Live chat and customer support	USA	EU-U.S. DPF / SCCs
9	Cloudflare, Inc.	CDN, DNS and network security	EU / USA	EU-U.S. DPF / SCCs
10	FD Transfers LLC (NOWPayments)	Cryptocurrency payment processing	Saint Vincent and the Grenadines	SCCs
11	Slack Technologies LLC	Optional notification channel (Controller-operated webhook)	USA	SCCs
12	Discord Inc.	Optional notification channel (Controller-operated webhook)	USA	EU-U.S. DPF / SCCs
13	Telegram FZ-LLC	Optional notification channel (Controller-operated bot/webhook)	United Arab Emirates	Channel selected and operated by the Controller

Note 1. Notification channels. Notification channels (Slack, Discord, Telegram and any webhook endpoint) are activated only where the Controller has configured them in its account, including the level of detail to be transmitted (asset-level alert with no credential payload, or full credential detail). Where the Controller routes credential-level notifications to a channel of its choice, it acts as the operator of that channel and remains responsible for the lawfulness of the resulting onward processing, including any international transfer mechanism for channels not operated within the EEA.

Note 2. Restricting credential-level detail to EEA channels. Where the Controller wishes credential-level notifications (plaintext passwords or password hashes) to be delivered only to EEA-located destinations, the Controller configures its own account accordingly: it selects email and/or webhook endpoints it operates within the EEA, and refrains from activating channels (such as Telegram, Discord or Slack) for credential-level payloads. The Processor does not pre-validate, restrict or geolocate the destinations chosen by the Controller.

Note 3. Updates. The exact corporate entity, country of establishment, and applicable transfer mechanism for each sub-processor may be confirmed on request. The Processor will notify the Controller of any addition or replacement of sub-processors at least thirty (30) days in advance, in accordance with Section 6.2 of the DPA, giving the Controller the opportunity to object.

Annex 3. Technical and Organisational Security Measures

Pursuant to Article 32 GDPR, the Processor implements the following technical and organisational measures, appropriate to the nature, scope and purpose of the processing carried out for the Controller and to the risks for the rights and freedoms of natural persons.

Encryption and data transmission

- Encryption of data in transit using TLS 1.3 for all connections to the Service, its API, and between infrastructure components.
- Encryption of all backups at rest using AES-256.
- Login passwords stored as salted cryptographic hashes (bcrypt cost 12); plaintext passwords are not retained.

At-rest protection of production storage (compensating control set)

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.

Access control and authentication

- Role-based access controls restricting access to personal data to authorised personnel on a need-to-know basis.
- Multi-factor authentication (MFA) enforced on administrative and infrastructure access.
- Periodic review of access rights; removal of access on personnel changes.

Infrastructure and segregation

- All Controller account and monitoring data hosted within EU/EEA data centres (France and Finland).
- Logically isolated production environments separated from development and testing environments.
- Dedicated infrastructure; production database not exposed to the public internet.

Resilience and continuity

- Regular encrypted backups of production data to support availability and restoration.
- Monitoring and logging of access and system events.

- Documented incident response procedure including breach notification under Section 8.

Organisational measures

- Confidentiality commitments binding all personnel with access to personal data.
- Engagement of sub-processors only under contractual data-protection obligations equivalent to those in this DPA.
- Periodic review of technical and organisational measures.