

# Data Processing Agreement

Version 1.0 — Effective 19 April 2026

This Data Processing Agreement (“**DPA**”) forms part of the agreement between SurfRank and the Customer for the provision of the Services (the “**Principal Agreement**”). It reflects the Parties’ agreement on the processing of Personal Data when the Customer uses the Services.

---

## 1. The Parties

---

**Processor:** SURF RANK PRIVATE LIMITED (“**SurfRank**”), a private limited company incorporated in Singapore with Unique Entity Number (UEN) 202613085N, having its registered office at **10 Marina Boulevard, #39-01, Marina Bay Financial Centre, Singapore 018983**. Contact: [privacy@surfrank.ai](mailto:privacy@surfrank.ai)

**Controller:** The Customer, as identified in the Principal Agreement (the “**Customer**”).

Each a “**Party**” and together the “**Parties**”.

---

## 2. Background and purpose

---

SurfRank provides an AI Search Intelligence and Answer Engine Optimization platform (the “**Services**”). In the course of providing the Services, SurfRank processes Personal Data on behalf of the Customer. This DPA sets out the terms on which SurfRank processes such Personal Data and gives effect to the Parties’ obligations under Applicable Data Protection Law, including in particular Article 28 of the GDPR.

---

## 3. Definitions

---

Terms used but not defined in this DPA have the meanings given in the Applicable Data Protection Law. In addition:

- “**Applicable Data Protection Law**” means, as applicable to a Party’s processing activities under this DPA, (a) Regulation (EU) 2016/679 (the “**GDPR**”); (b) the GDPR as incorporated into UK law by the Data Protection Act 2018 (the “**UK GDPR**”); (c) the Singapore Personal Data Protection Act 2012 (the “**PDPA**”); (d) the California Consumer Privacy Act, as amended (the “**CCPA**”); and (e) any other applicable data protection or privacy law.

- “**Customer Personal Data**” means Personal Data that SurfRank processes on behalf of the Customer under the Principal Agreement, as described in Annex I.B.
- “**EU SCCs**” means the Standard Contractual Clauses set out in Commission Implementing Decision (EU) 2021/914.
- “**UK IDTA**” means the International Data Transfer Agreement (or the UK Addendum to the EU SCCs) issued by the UK Information Commissioner under s.119A of the UK Data Protection Act 2018.
- “**Personal Data Breach**” has the meaning given in the GDPR and includes any equivalent term under other Applicable Data Protection Law.
- “**Sub-processor**” means any processor engaged by SurfRank to process Customer Personal Data.

Capitalised terms used for “Controller”, “Processor”, “Personal Data”, “Processing”, “Data Subject” and “Supervisory Authority” have the meanings given in the GDPR.

---

## 4. Roles and responsibilities

---

4.1 The Parties acknowledge that, for the purposes of Applicable Data Protection Law, the Customer is the **Controller** and SurfRank is the **Processor** with respect to the Customer Personal Data.

4.2 Each Party shall comply with its obligations under Applicable Data Protection Law. The Customer is solely responsible for the accuracy, quality and legal basis of Customer Personal Data and the means by which the Customer acquired that data.

4.3 The Customer’s documented instructions to SurfRank are (i) to process Customer Personal Data as necessary to provide the Services in accordance with the Principal Agreement, this DPA, and the Customer’s use of the Services; and (ii) any additional written instructions agreed in writing by the Parties. SurfRank will immediately inform the Customer if, in its opinion, an instruction infringes Applicable Data Protection Law.

---

## 5. Subject matter, nature and duration of processing

---

The subject matter, nature, purpose, types of Personal Data and categories of Data Subjects processed under this DPA, and the duration of the processing, are set out in **Annex I.B.**

Processing will continue for the duration of the Principal Agreement and thereafter only to the extent and for the period required by applicable law or as specifically instructed by the Customer.

---

## 6. Obligations of SurfRank

---

SurfRank shall:

**6.1 Process only on documented instructions.** Process Customer Personal Data only on documented instructions from the Customer, including with regard to transfers of Personal Data to a third country, unless required to do so by applicable law. In that case, SurfRank shall inform the Customer of that legal requirement before processing, unless the law prohibits such disclosure on important grounds of public interest.

**6.2 Confidentiality.** Ensure that persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

**6.3 Security.** Implement the technical and organisational measures set out in **Annex II** and such further measures as are required by Applicable Data Protection Law (including Article 32 GDPR) to ensure a level of security appropriate to the risk.

**6.4 Sub-processors.** Only engage Sub-processors in accordance with Section 8 below.

**6.5 Assistance with Data Subject Rights.** Taking into account the nature of the processing, assist the Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling the Customer's obligation to respond to requests from Data Subjects to exercise their rights under Applicable Data Protection Law. Where a Data Subject contacts SurfRank directly in respect of Customer Personal Data, SurfRank shall promptly forward the request to the Customer and shall not respond to the Data Subject except on the Customer's instructions or as required by law.

**6.6 Assistance with other Controller obligations.** Assist the Customer in ensuring compliance with the obligations under Articles 32 to 36 of the GDPR, taking into account the nature of the processing and the information available to SurfRank (including security, breach notification, data protection impact assessments and prior consultations with supervisory authorities).

**6.7 Deletion or return.** At the choice of the Customer, delete or return all Customer Personal Data to the Customer after the end of the provision of the Services, and delete existing copies unless applicable law requires storage of the Personal Data. See Section 12.

**6.8 Records and audits.** Make available to the Customer all information necessary to demonstrate compliance with Article 28 GDPR and this DPA, and allow for and contribute to audits in accordance with Section 11.

**6.9 Privacy by design.** Have regard to the principles of data protection by design and by default in the development and operation of the Services.

---

## **7. International transfers**

---

**7.1 EU transfers.** Where processing under this DPA involves a transfer of Personal Data from the European Economic Area to a country outside the EEA that is not subject to an adequacy decision, the EU SCCs are incorporated into this DPA by reference and apply to such transfer as follows:

(a) Module Two (Controller to Processor) applies where the Customer is a Controller and SurfRank is a Processor;  
(b) Module Three (Processor to Processor) applies where the Customer is a Processor and SurfRank is a Sub-processor; © Clause 7 (docking clause) is included; (d) Option 2 of Clause 9(a) (general written authorisation for

Sub-processors) applies, with the time period in Section 8.2 below; (e) Clause 11(a) — the optional independent dispute resolution body is **not** used; (f) Clause 17 — the governing law is the law of **Ireland**; (g) Clause 18 — disputes are resolved before the courts of **Ireland**; (h) Annex I, II and III to the EU SCCs are populated by Annex I.A, I.B, II and III of this DPA respectively.

**7.2 UK transfers.** Where processing involves a restricted transfer under the UK GDPR, the UK IDTA (or the UK Addendum to the EU SCCs) is incorporated into this DPA by reference, with the EU SCCs as varied above forming the “Approved EU SCCs” for the purposes of the UK Addendum.

**7.3 Other jurisdictions.** Where Applicable Data Protection Law requires an equivalent transfer mechanism for restricted transfers from other jurisdictions (including Switzerland), the Parties shall cooperate in good faith to put in place such mechanism.

---

## 8. Sub-processors

---

**8.1 General authorisation.** The Customer provides SurfRank with general written authorisation to engage the Sub-processors listed in **Annex III** for the processing of Customer Personal Data.

**8.2 Changes.** SurfRank maintains an up-to-date list of Sub-processors at <https://surfrank.ai/trust/> and will notify the Customer of any intended addition or replacement of a Sub-processor at least thirty (30) days before the change takes effect. The Customer may object to any such change on reasonable data protection grounds within that notice period. If the Parties cannot agree on a resolution, the Customer may terminate the affected part of the Services for convenience without penalty by giving written notice.

**8.3 Sub-processor obligations.** SurfRank shall impose on each Sub-processor, by way of a written contract, data protection obligations materially equivalent to those set out in this DPA, including in particular providing sufficient guarantees to implement appropriate technical and organisational measures. SurfRank remains fully liable to the Customer for the performance of any Sub-processor’s obligations.

---

## 9. Personal Data Breach

---

**9.1 Notification to Customer.** SurfRank shall notify the Customer without undue delay, and in any event within **seventy-two (72) hours**, after becoming aware of a Personal Data Breach affecting Customer Personal Data.

**9.2 Contents of notification.** The notification shall include, to the extent reasonably available to SurfRank at the time:

(a) a description of the nature of the breach including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (b) the name and contact details of SurfRank’s point of contact where more information can be obtained; (c) a description of the likely consequences of the breach; and (d) a description of the measures taken or proposed to address the breach and mitigate its possible adverse effects.

Where it is not possible to provide all information at once, SurfRank may provide it in phases without further undue delay.

9.3 **Assistance.** SurfRank shall cooperate with the Customer and take reasonable commercial steps as directed by the Customer to assist in the investigation, mitigation and remediation of the Personal Data Breach.

9.4 **Direct notifications.** SurfRank shall not notify any Data Subject, Supervisory Authority or other third party of a Personal Data Breach on the Customer's behalf without the Customer's prior written consent, unless required by applicable law.

---

## 10. Data Protection Impact Assessments

---

Taking into account the nature of processing and the information available, SurfRank shall provide reasonable assistance to the Customer with any data protection impact assessments and prior consultations with Supervisory Authorities which the Customer reasonably considers to be required under Articles 35 or 36 GDPR or equivalent provisions.

---

## 11. Audits

---

11.1 **Information rights.** SurfRank shall make available to the Customer information reasonably necessary to demonstrate compliance with this DPA. Such information shall be provided primarily through: (a) SurfRank's published security documentation, including the Trust page at <https://surfrank.ai/trust/>, this DPA, and the current Sub-processor list; and (b) written responses to the Customer's reasonable security and privacy questionnaires, provided within a reasonable timeframe.

11.2 **Third-party certifications.** Where SurfRank has obtained an independent third-party certification or audit report (such as SOC 2 or ISO 27001, or any equivalent industry-recognised standard), SurfRank may satisfy the Customer's audit rights under this Section 11 by providing a copy of the most recent such report under an appropriate confidentiality undertaking. SurfRank's current certification status is published at <https://surfrank.ai/trust/>.

11.3 **On-site audits.** On-site audits or audits conducted by an independent auditor mandated by the Customer (the "**Auditor**") shall only be required where (i) the information provided under Sections 11.1 and 11.2 is reasonably insufficient to demonstrate SurfRank's compliance; (ii) the Customer provides at least thirty (30) days' prior written notice; (iii) the audit is conducted no more than once in any 12-month period, save where required by a Supervisory Authority or following a Personal Data Breach; (iv) the audit takes place during normal business hours, with minimum disruption to SurfRank's business, in accordance with SurfRank's reasonable security and confidentiality requirements, and at the Customer's expense; and (v) the Auditor is not a competitor of SurfRank and is bound by written confidentiality obligations equivalent to those in the Principal Agreement.

---

## 12. Return or deletion of Customer Personal Data

---

12.1 Upon termination or expiry of the Principal Agreement, and at the Customer's choice expressed in writing within thirty (30) days of such termination or expiry, SurfRank shall either:

(a) return all Customer Personal Data in a commonly-used, machine-readable format; or (b) delete all Customer Personal Data from its systems, including from Sub-processors' systems.

12.2 If the Customer does not make an election within thirty (30) days, SurfRank shall delete all Customer Personal Data.

12.3 Backup copies and data retained for legal, regulatory or audit purposes may be retained for the period required by applicable law, provided that such data remains subject to the confidentiality and security obligations of this DPA.

12.4 On completion, SurfRank shall provide written confirmation of deletion or return on request.

---

## 13. Liability

---

13.1 Each Party's aggregate liability arising out of or related to this DPA, whether in contract, tort (including negligence) or under any other theory of liability, shall not exceed the **total fees paid or payable by the Customer to SurfRank under the Principal Agreement in the twelve (12) months immediately preceding the event giving rise to the claim**. Any reference in the Principal Agreement to the liability of a Party means the aggregate liability of that Party under the Principal Agreement and this DPA taken together, and this DPA shall not give rise to any separate or additional liability cap.

13.2 Nothing in this DPA limits or excludes either Party's liability where such limitation or exclusion is not permitted by Applicable Data Protection Law, including liability owed directly to a Data Subject under Article 82 GDPR.

---

## 14. General

---

14.1 **Order of precedence.** In the event of a conflict between this DPA and the Principal Agreement, this DPA prevails in respect of the processing of Personal Data. In the event of a conflict between this DPA and the EU SCCs or UK IDTA, the EU SCCs or UK IDTA prevail.

14.2 **Amendments.** SurfRank may update this DPA from time to time where reasonably required to reflect changes in Applicable Data Protection Law, guidance from Supervisory Authorities, or changes in the Services. Any material change will be notified to the Customer with at least thirty (30) days' prior notice.

14.3 **Severability.** If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions remain in full force and effect.

14.4 **Governing law and jurisdiction.** This DPA is governed by the laws of the **Republic of Singapore**. The courts of **Singapore** have exclusive jurisdiction over any dispute arising out of or in connection with this DPA, subject to Section 7 in respect of the EU SCCs and the UK IDTA.

14.5 **Counterparts and electronic signature.** This DPA may be executed in counterparts and by electronic signature, each of which is deemed an original.

---

## Signatures

---

### For SurfRank:

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

### For the Customer:

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

---

# Annex I.A — List of Parties

**Data Exporter (Controller):** The Customer, as identified in the Principal Agreement.

- Contact: as set out in the Principal Agreement.
- Activities relevant to the transfer: use of the Services as Customer.
- Role: Controller (or Processor, where the Customer is itself a Processor acting on behalf of its own controllers).

**Data Importer (Processor):** SURF RANK PRIVATE LIMITED

- UEN: 202613085N
  - Address: 10 Marina Boulevard, #39-01, Marina Bay Financial Centre, Singapore 018983
  - Contact: [privacy@surfrank.ai](mailto:privacy@surfrank.ai)
  - Activities relevant to the transfer: provision of AI Search Intelligence and Answer Engine Optimization services, including brand visibility analysis across third-party AI engines.
  - Role: Processor (or Sub-processor where Module Three applies).
-

# Annex I.B — Description of the Processing

## Categories of Data Subjects whose Personal Data is processed:

- The Customer's authorised users (employees, contractors) who access the Services (administrators, editors, viewers).
- The Customer's end-customers, prospects or audiences, to the extent the Customer inputs their Personal Data into the Services (e.g. a name appearing in an article drafted in Article Studio).
- Individuals named or identifiable in content submitted to or generated by the Services (e.g. authors of webpages analysed, individuals referenced in generated articles).

## Categories of Personal Data processed:

- **Account data:** name, work email address, hashed password, role, workspace membership, profile image URL.
- **Authentication data:** Firebase Auth identifiers, session tokens, IP addresses, user-agent strings, API key hashes.
- **Usage and telemetry data:** product events, page views, feature interactions, error logs, timestamps.
- **Customer-submitted content:** website URLs, keywords, competitor domains, uploaded brand materials, drafted articles, natural-language prompts.
- **Integration credentials:** encrypted OAuth tokens and API tokens for integrations the Customer authorises (e.g. Google Analytics 4, WordPress, Shopify, Webflow, Ghost).
- **Billing data:** company name, billing address, plan, invoice history. Payment card numbers are collected and processed by Stripe and are **not** stored by SurfRank.
- **Support data:** contents of support emails, tickets or chat messages.

**Special categories of Personal Data:** SurfRank does not intentionally process special categories of Personal Data (Article 9 GDPR). The Customer shall not submit special-category Personal Data to the Services unless expressly agreed in writing.

**Nature of the processing:** collection, recording, organisation, structuring, storage, retrieval, consultation, use, transmission to Sub-processors, analysis (including by automated means), generation of reports and derived content, deletion.

**Purpose of the processing:** providing the Services as described in the Principal Agreement, including: AI visibility scoring across multiple AI engines; competitor tracking; content-gap and opportunity analysis; article generation; publishing integrations; account administration; billing; and security, fraud prevention and diagnostic purposes.

**Duration of the processing:** for the duration of the Principal Agreement, plus any retention period required by applicable law or agreed in writing (see Section 12).

**Frequency of the transfer:** continuous, on Customer-initiated basis.



# Annex I.C — Competent Supervisory Authority

Because SurfRank (the data importer) is not established in the European Union, the competent Supervisory Authority for the purposes of Clause 13 of the EU SCCs is determined by reference to the data exporter (Customer). Where the data exporter is established in an EU Member State, the competent Supervisory Authority is the Supervisory Authority of that Member State. Where the data exporter is not established in the EU but falls within the territorial scope of Article 3(2) GDPR, the competent Supervisory Authority is that of the Member State in which the data exporter's representative pursuant to Article 27(1) GDPR is established. Where the data exporter is not subject to the GDPR, the competent Supervisory Authority is that of the Member State in which the Data Subjects whose Personal Data is transferred under the EU SCCs are located.

**Default:** unless otherwise agreed in writing, the Parties designate the **Irish Data Protection Commission (Dublin, Ireland)** as the competent Supervisory Authority for EU SCC purposes.

For processing activities subject to the Singapore Personal Data Protection Act, the competent authority is the **Personal Data Protection Commission (PDPC) of Singapore**.

---

# Annex II — Technical and Organisational Measures

SurfRank implements and maintains the following technical and organisational measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (Article 32 GDPR). This Annex is aligned with the measures published at <https://surfrank.ai/trust/>.

## 1. Encryption

- **In transit:** all traffic to and from the Services uses TLS 1.3 with modern cipher suites. HSTS is enforced on all subdomains.
- **At rest:** Firestore encrypts all stored data with AES-256. Sensitive secrets (API tokens, OAuth credentials) are additionally encrypted with per-tenant AES-256-GCM keys before being written to storage.
- **Backups:** backups are encrypted with the same key management.

## 2. Access control and authentication

- Authentication is built on Firebase Auth. Plaintext passwords are never stored by SurfRank.
- API keys issued by SurfRank are hashed with SHA-256 before storage; SurfRank can revoke keys but cannot read them.
- Internal access to production systems is role-based, requires multi-factor authentication, and is logged.
- The principle of least privilege is enforced; access is reviewed periodically.

## 3. Pseudonymisation and data minimisation

- Personal Data is processed only to the extent necessary for the stated purpose.
- Where practicable, identifiers are replaced with internal IDs when used in logs and analytics.
- Data retention is configured per data type, with automatic deletion where feasible.

## 4. Resilience and availability

- Production infrastructure is hosted on Hetzner (EU, Germany) with Cloudflare providing DNS, TLS termination and DDoS protection.
- Daily automated backups with tested restore procedures.
- Monitoring and alerting on uptime, error rates and suspicious activity.

## 5. Change management and secure development

- Source code is version-controlled; all changes go through peer review.
- Dependencies are monitored for known vulnerabilities and patched on a risk-prioritised basis.
- Production deployments run from audited, reproducible build environments.

## **6. Incident response**

- Documented incident response procedure covering detection, triage, containment, eradication, recovery and post-incident review.
- Personal Data Breach notifications in line with Section 9 of this DPA.

## **7. Personnel**

- All personnel with access to Customer Personal Data are bound by confidentiality obligations and receive data protection training.
- Access is revoked promptly on termination or role change.

## **8. Sub-processor governance**

- Sub-processors are evaluated prior to engagement for security and privacy maturity.
- Sub-processors are contractually bound to equivalent security and privacy standards.
- The Sub-processor list is maintained at <https://surfrank.ai/trust/>.

## **9. Data subject rights tooling**

- The Services provide self-service tooling for account holders to export, correct and delete their own Personal Data.
- The Customer can request assistance with broader Data Subject requests via [privacy@surfrank.ai](mailto:privacy@surfrank.ai).

## **10. Physical security**

- SurfRank does not operate its own data centres. Physical security is the responsibility of the Sub-processors named in Annex III, each of which maintains industry-standard physical security controls at the facilities used to provide the Services.
-

# Annex III — List of Approved Sub-processors

As of the effective date of this DPA, SurfRank engages the following Sub-processors. The current list is maintained at <https://surfrank.ai/trust/>.

#	Sub-processor	Entity & location	Processing activity	Data location
1	<b>Google LLC / Google Ireland Limited</b> (Firebase, Google Cloud)	US / Ireland	Authentication (Firebase Auth), Firestore database, Cloud Storage, Cloud Messaging	US / EU
2	<b>Hetzner Online GmbH</b>	Germany	Application hosting (API, background workers, MCP server)	EU (Germany)
3	<b>Cloudflare, Inc.</b>	US	DNS, TLS termination, DDoS protection, CDN	Global (edge)
4	<b>Anthropic, PBC</b>	US	Claude AI processing of Customer-initiated queries	US
5	<b>OpenAI, L.L.C.</b>	US	GPT AI processing of Customer-initiated queries	US
6	<b>Google Ireland Limited</b> (Gemini API)	Ireland / US	Gemini AI processing of Customer-initiated queries	US / EU
7	<b>xAI Corp.</b> (Grok)	US	Grok AI processing of Customer-initiated queries	US
8	<b>Perplexity AI, Inc.</b>	US	Perplexity AI processing of Customer-initiated queries	US
9	<b>DeepSeek (Hangzhou DeepSeek Artificial Intelligence Co., Ltd.)</b>	China	DeepSeek AI processing of Customer-initiated queries	China
10	<b>Groq, Inc.</b> (serving Meta Llama models)	US	Meta AI / Llama model processing of Customer-initiated queries	US
11	<b>Stripe, Inc. / Stripe Payments Europe, Ltd.</b>	US / Ireland	Payment processing; Stripe is an independent Controller for payment data	Global
12	<b>Transactional email provider</b> (as listed on <a href="https://surfrank.ai/trust/">surfrank.ai/trust/</a> )	US / EU	Transactional email delivery (account verification, notifications, billing receipts)	US / EU

**Notes on AI engine sub-processors (rows 4–10):** SurfRank transmits only the minimum content necessary to execute the Customer’s requested query (typically: the keyword or prompt, and — where explicitly configured — a brand or domain name). Responses are stored in the Customer’s workspace in Firestore. Where the underlying

AI provider offers zero-retention or non-training API tiers, SurfRank uses those tiers where commercially available.

---

*The Customer and SurfRank may negotiate specific amendments prior to signature. Last updated: 19 April 2026.*