

# DATA PROCESSING AGREEMENT

This Data Processing Agreement (the “Agreement”) forms part of the Terms and Conditions (the “T&Cs”)

between:

**[CONTROLLER LEGAL NAME]**, a company incorporated under the laws of **[COUNTRY]** with its registered office at **[ADDRESS]** (the “Controller”);

and

**Linkup Technologies SAS**, a company incorporated under the laws of France, having its registered office at 28 avenue des Pépinières, 94260 Fresnes, France, registered with the Créteil Trade and Companies Register under number 930 910 740 (“Linkup” or the “Processor”).

The Controller and the Processor are each a “Party” and together the “Parties”.

**Effective date:** **[DATE]**

## 1. Definitions and Interpretation

Capitalised terms not otherwise defined in this Agreement have the meaning given to them in Regulation (EU) 2016/679 (“GDPR”). The terms *Affiliate*, *Personal Data*, *Processing*, *Sub-processor*, *Data Subject*, *Personal Data Breach*, *Supervisory Authority* and *Standard Contractual Clauses* (or “SCCs”) shall be interpreted in accordance with the GDPR. “EU Data Protection Law” means the GDPR and any national law supplementing it.

## 2. Subject-matter, Nature, Purpose and Duration of the Processing

### 2.1 Subject-matter & Purpose.

The Processor will process Personal Data solely (i) to provide the services described in the T&Cs (“Services”); (ii) to comply with documented instructions of the Controller; and (iii) to maintain, secure, and improve the Services, including by creating anonymised and aggregated data that no longer identifies any Data Subject.

**2.2 Nature of Processing.** The Services primarily consist of AI-powered search, analytics and customer-support tooling delivered via web APIs and related interfaces.

**2.3 Data Retention. (a) Personal Data:** Queries, answers, and any Personal Data shall be deleted immediately upon completion of each API request. **(b) Usage Metadata:** Anonymized technical metadata (API call volumes, transaction type, dates, API Keys) may be retained for service optimization and billing purposes.

**2.4 Instructions.** This Agreement constitutes the Controller's complete and final instructions to Processor. Additional instructions must be agreed in writing and may be subject to additional fees if they require material effort beyond the standard Services.

**2.5 Anonymised Data.** Data rendered anonymous in accordance with Recital 26 GDPR is not Personal Data. The Processor may freely process such anonymised data.

### **3. Controller Responsibilities**

The Controller shall (a) ensure that it has a valid legal basis for the Processing, (b) not instruct the Processor to process Personal Data in a manner that breaches EU Data Protection Law, and (c) remain solely responsible for the accuracy, quality and legality of Personal Data provided to the Processor.

### **4. Confidentiality and Personnel**

4.1 The Processor ensures that all personnel authorised to process Personal Data are subject to an appropriate statutory or contractual duty of confidentiality.

4.2 The Processor shall take reasonable steps to ensure the reliability of such personnel and to limit access to Personal Data on a need-to-know basis.

### **5. Security of Processing**

5.1 The Processor shall implement and maintain the technical and organisational measures described in **Annex II** (the "TOMs"), designed to protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction or damage, as required by Article 32 GDPR.

5.2 The Processor may update the TOMs from time to time provided that such updates do not materially reduce the overall level of protection for Personal Data.

## **6. Sub-processing**

**6.1 General Authorisation.** The Controller grants Processor a general written authorisation to engage Sub-processors listed in **Annex III** and any future Sub-processors in accordance with this Section 6.

**6.2** The Processor shall impose data-protection obligations on each Sub-processor that are no less protective than those set out in this Agreement.

**6.3** The Processor will notify the Controller at least thirty (30) days in advance of any intended addition or replacement of Sub-processors. The Controller may object on reasonable, data-protection-related grounds within fifteen (15) days of notification. If the Controller does not object within that period, the Sub-processor shall be deemed approved.

**6.4** Where a Sub-processor fails to fulfil its data-protection obligations, the Processor shall remain liable to the Controller for the performance of that Sub-processor's obligations in accordance with Section 11 (Liability).

## **7. International Data Transfers**

**7.1** The Processor shall not transfer Personal Data outside the European Economic Area ("EEA") unless it has ensured an adequate level of protection in compliance with Chapter V GDPR.

**7.2** Transfers to Sub-processors in non-EEA countries shall rely on the EU Standard Contractual Clauses for the transfer of personal data to third countries (Commission Implementing Decision (EU) 2021/914), module 2 (controller-to-processor), which are hereby incorporated by reference and shall automatically apply between the Controller and each relevant Sub-processor.

## **8. Assistance to the Controller**

**8.1 Data Subject Requests.** Taking into account the nature of the Processing, the Processor shall assist the Controller, by appropriate technical and organisational measures and insofar as commercially reasonable, to respond to Data Subject requests under Chapter III GDPR. Where such assistance incurs more than a minimal cost, the Processor may charge the Controller on a time-and-materials basis.

**8.2 Impact Assessments & Consultation.** The Processor shall, upon request, provide

the Controller with reasonable assistance to conduct data-protection impact assessments and prior consultations with Supervisory Authorities, solely to the extent that such assistance is not already available through the Services and insofar as it relates to the Processing of Controller Personal Data.

## **9. Audits and Compliance Information**

9.1 **Third-party Reports.** Processor shall annually procure an independent report covering the security controls relevant to the Services and shall provide a summary of such report to Controller upon written request.

9.2 **Questionnaire.** Where the summary report demonstrates material deficiencies, Controller may submit a written security questionnaire (max. 50 questions) to which Processor shall respond in writing within a reasonable time.

9.3 **On-site Audit.** Only if (i) required by a Supervisory Authority or (ii) the foregoing measures prove insufficient to demonstrate compliance, the Controller may, no more than once in any rolling twelve-month period, conduct an on-site inspection on thirty (30) days' notice during normal business hours.

Controller shall

- (a) be strictly limited to areas where Personal Data is processed,
- (b) comply with Processor's reasonable confidentiality and security policies, and
- (c) bear all costs (including Processor's reasonable internal costs) associated with the audit.

9.4 Audits shall not provide access to other customers' data, proprietary algorithms, source code or trade secrets.

## **10. Personal Data Breach**

The Processor shall notify the Controller without undue delay and, where feasible, within forty-eight (48) hours after becoming aware of a Personal Data Breach affecting Controller Personal Data. The notification shall describe, to the extent known, the nature of the breach, the likely consequences and the measures taken or proposed to address it.

## **11. Liability**

11.1 Processor's aggregate liability arising under or in connection with this Agreement, whether in contract, tort (including negligence) or otherwise, shall be limited to the total amounts paid or payable by Controller to Processor pursuant to the T&Cs in the twelve (12) months preceding the event giving rise to liability.

11.2 Neither Party shall be liable for any indirect, incidental or consequential damages, including lost profits or revenue, loss of data or business interruption, except to the extent that such limitation is prohibited by applicable law.

11.3 Except where prohibited by mandatory law (including Article 82 GDPR), the Parties' liability obligations under this DPA shall be subject to the liability limitations and exclusions set forth in the Main Service Agreement between the parties

11.4 Nothing in this Agreement limits a Party's liability for (a) death or personal injury caused by its negligence, (b) its wilful misconduct or gross negligence, or (c) any liability that cannot lawfully be limited.

## **12. Return and Deletion of Data**

Upon termination or expiry of the T&Cs, Controller may instruct Processor to (a) return all Personal Data in a commonly used, machine-readable format, or (b) securely delete it. Processor shall comply within thirty (30) days, save that Personal Data may remain in routine backups until overwritten, and provided that retention is not required by EU or Member-State law.

## **13. Miscellaneous**

**Order of Precedence.** In the event of any conflict between this Agreement and the T&Cs, this Agreement shall prevail with respect to data-protection matters.

**Governing Law & Jurisdiction.** This Agreement shall be governed by the laws of France. The courts of Paris, France shall have exclusive jurisdiction, unless mandatory law requires otherwise.

**Severability.** Should any provision of this Agreement be invalid or unenforceable, the remaining provisions shall remain in full force and effect.

**Entire Agreement; Amendments.** This Agreement may only be amended by a written instrument signed by both Parties.

**Notices.** All notices under this Agreement shall be sent by email to the contact persons notified in writing.

IN WITNESS WHEREOF, the parties have executed this Addendum as of the date last signed below

**For** \_\_\_\_\_ **Controller For Linkup Technologies SAS**

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

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

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

# Annex I – Details of Processing

Item	Description
<b>Data-subject categories</b>	End-users of the Controller’s application whose search / chat queries are sent to Linkup’s API Controller employees or contractors who open support tickets Controller’s billing and commercial contacts
<b>Categories of personal data</b>	User-supplied content: free-text search or chat queries and the corresponding answers that may contain personal data Technical metadata: IP address, browser/OS details, timestamps, request/response identifiers and error traces Business-contact data: name, job title, email, phone and postal/billing address Support material: ticket text and attachments
<b>Purpose(s) of processing</b>	(i) Provision, maintenance and security of Linkup’s AI search & analytics services; (ii) customer support and incident resolution; (iii) usage statistics and fraud prevention ; (iv) billing and account management.
<b>Nature of processing</b>	Collection, storage, structuring, analysis, retrieval, transmission, erasure and destruction, as necessary to deliver the Services.
<b>Retention schedule</b>	<b>Query and answer corpus:</b> retained for the duration of the Main Services Agreement and thereafter <b>until the Controller instructs deletion</b> , enabling long-term search history, analytics and model improvement. <b>Technical logs (IP, error traces):</b> automatically deleted after <b>14 days</b> . <b>Support-ticket history: 3 years</b> after ticket closure . <b>Business-contact data: 5 years</b> after the end of the contractual relationship. <b>Encrypted backups: 30-day</b> rolling purge.
<b>Frequency &amp; method</b>	Continuous, on-demand API calls initiated by the Controller’s systems.
<b>Processing locations</b>	All production systems and backups are hosted in <b>Microsoft Azure EU regions</b> (e.g. West Europe, North Europe).

# **Annex II - Technical & Organisational Measures (TOMs)**

## **1. Governance & Certification**

- SOC 2 Type II compliance in progress (Q4 2025 target completion)
- Data-protection officer appointed (Philippe Mizrahi); governance council reviews.

## **2. Access Control**

- SSO & MFA enforced for all staff accounts.
- Role-based permissions (least privilege); quarterly entitlement reviews.
- Production access restricted to vetted engineering personnel; actions logged via comprehensive audit logs.

## **3. Encryption**

- TLS 1.2+/HTTPS for data in transit.
- AES-256 encryption at rest for databases, object storage and backups (Azure Key Vault managed keys).
- Customer-specific API tokens stored salted & hashed.

## **4. Physical & Environmental Security**

- Hosting in Azure data centers with SOC-2 compliance and comprehensive physical security.
- Linkup offices secured by key-card plus alarm; paperless operations.

## **5. System Security & Hardening**

- Hardened base images, automatic OS patching.
- Anti-malware across endpoints; container image scanning.
- WAF + DDoS mitigation (Azure-native protections).

## **6. Network Security**

- VPC segregation; sub-nets for web, app, DB tiers; no public DB endpoints.
- Network segmentation using Azure Security Groups and NACLs.
- VPN-only administrative access.

## **7. Monitoring & Incident Response**

- 24×7 incident response capability; structured severity-based escalation (S1-S4).
- Documented incident-response plan; annual tabletop testing.
- Breach notification procedure: 24-48 hours to Controller.

## **8. Business Continuity & Disaster Recovery**

- 30-day backup retention; Azure-native backup solutions.
- Cross-region capabilities available.
- Annual restore tests.

## **9. Supplier & Sub-processor Management**

- Limited subprocessor chain: Microsoft Azure (France), Google Workspace (EU), GitHub (EU).
- All subprocessors SOC 2/equivalent certified.

## **10. Employee Security & Awareness**

- Background checks for positions of trust.
- Mandatory GDPR & security training