Privacy Policy – Brainqub3 Fact Checker

Effective date: 13 October 2025
Application domain: https://check.brainqub3.com/

1) Who we are

DATA-CENTRIC SOLUTIONS LTD (trading as **Brainqub3**)
Company number: **14829432**
Registered office: **86–90 Paul Street, London, England, United Kingdom, EC2A 4NE**
("**Brainqub3**", "**we**", "**us**", "**our**")

Contact for privacy matters: **privacy@brainqub3.com**

2) Scope of this notice

This privacy policy explains how we handle personal data when you:

- visit or use **Brainqub3 Fact Checker** at **https://check.brainqub3.com/**;
- create and manage an account or make payments; or
- submit text and documents to be fact-checked ("**Customer Content**").

We comply with the **UK GDPR**, the **Data Protection Act 2018**, and—where we target or serve individuals in the EEA—the **EU GDPR** and applicable local laws.

3) Our roles (Controller vs Processor)

- **Processor (Customer Content):** For text, files and other content you submit to the fact-checking service, we act as your **data processor**. You are the **data controller** and determine the purposes and means of processing. We process Customer Content only on your documented instructions, under our terms and any applicable data processing addendum (DPA).
- **Controller (account, billing, website & payments):** For account registration, billing and payments (via Stripe), service communications, security logging and our websites, we act as an **independent controller**.

If you are a business customer and need a signed **DPA**, please contact us.

4) The data we process

A) Customer Content (processor role)

- **What:** The text and documents you upload to be fact-checked, plus derived output necessary to provide results.
- **Where stored:** In **Supabase Storage (UK)** while the job runs. We **delete uploaded documents after the job completes**. Short-lived backups or caching

maintained by our providers may persist briefly and are then purged according to their schedules.

B) Account, billing & support data (controller role)

- **Identification: Full name, email address** (as provided by you).
- **Payments:** Payment-related information and transaction metadata processed via **Stripe** (see Section 6). **We do not store or have access to full card numbers or CVC; these are collected and processed securely by Stripe.**
- **Authentication & security:** Credentials, session identifiers, IP address, device/usage information needed to protect the service.
- **Support & communications:** Content of messages you send us (e.g., tickets, emails).

C) Technical & usage data (controller role)

- **Device and log data:** IP address, browser/OS information, timestamps, and activity logs necessary to operate, secure and troubleshoot the service.
- **Cookies/Local Storage:** Strictly necessary cookies for sign-in, payments, and session integrity; optional analytics cookies only if/when deployed (see **Cookies** below).

We do **not** intentionally collect special category data (e.g., health, biometric). If you include such data in Customer Content, you remain responsible as controller for having a lawful basis and appropriate safeguards.

5) Why we use personal data and legal bases

When we are Controller

- **Provide and administer accounts, authenticate users, process payments, deliver the service** (legal basis: **performance of a contract** or steps prior to entering a contract).
- **Fraud prevention, security and incident response** (legal basis: **legitimate interests** in running a secure, reliable SaaS; for payment fraud checks, we and Stripe rely on legitimate interests).
- **Communicate service updates, respond to support requests** (legal basis: **contract / legitimate interests**).
- **Comply with law (e.g., tax, accounting, financial regulations) and enforce terms** (legal basis: **legal obligation / legitimate interests**).

- **Analytics and product improvement** (legal basis: **legitimate interests**; where cookies are used, **consent** via the cookie banner/controls).

When we are Processor

- **Perform fact-checking and deliver outputs** strictly under your instructions (legal basis determined by you, the controller).

We **do not sell** personal information.

6) Sub-processors, payment processors and recipients

We use reputable providers to host and process data under appropriate contractual safeguards:

- **Supabase** – application database and storage
    - **Region:** UK
    - **Use:** Store application data to provide the fact-checking service; store uploaded documents while jobs run; documents are **deleted after completion**.
    - **Personal data processed:** account data (name, email), Customer Content, operational metadata.
- **OpenAI** – downstream data processor for generative AI inference
    - **Use:** Customer Content and prompts are sent to OpenAI to generate and verify outputs. Processing is governed by OpenAI's data processing terms, including their **Data Processing Addendum**: openai.com/policies/data-processing-addendum/
    - **Note:** Generative AI providers may process data in multiple regions. We restrict use to the extent available by contract and configuration and do not permit training on Customer Content beyond what is contractually agreed.
- **Fly.io** – application compute platform
    - **Region for our workloads:** London, UK
    - **Use:** Runs our backend application services and processing.
- **Stripe** – **payments** (card processing, fraud prevention, recurring billing)
    - **Use:** We use Stripe to collect and process payments. Stripe receives payment method details (e.g., card information), your name, email, billing address, device and technical data for fraud prevention, and transaction metadata.

- **Controller/processor role:** Stripe may act as an **independent controller** for parts of the processing necessary to provide its regulated payment services and fraud prevention, and as our **processor** for certain merchant services. See **Stripe's Privacy Policy** at **stripe.com/privacy** for details.
- **Data minimisation: We never receive or store full card numbers or CVC.** Those are submitted directly to Stripe (e.g., via Stripe Elements/Checkout) and tokenised.

Other disclosures: We may disclose data (a) to professional advisers (lawyers, accountants) under confidentiality duties; (b) to authorities where required by law; (c) in connection with a merger, acquisition or corporate reorganisation with appropriate safeguards.

Changes to (sub-)processors: We may update providers over time. For material changes affecting Customer Content or payments, we will post an update to this page and, where feasible, notify account owners prior to the change.

7) International transfers

Where personal data is transferred outside the UK/EEA (for example by **Stripe** or **OpenAI** or other providers operating globally), we rely on appropriate safeguards such as the **UK International Data Transfer Agreement**, the **EU Standard Contractual Clauses** plus the **UK Addendum**, and/or an applicable **adequacy decision**. Details are available on request.

8) Retention

- **Customer Content:** Uploaded documents are **deleted after the fact-checker job completes**. Derived outputs may be retained in your account only as necessary to provide the service you request.
- **Payments & billing:** Transaction records are retained as required for **tax and accounting compliance** and to manage chargebacks/disputes (typically up to **6 years** in the UK, subject to statutory requirements). Card details are not stored by us.
- **Account & support data:** Kept for the life of your account and then deleted or anonymised in accordance with our retention schedule and legal requirements.
- **Security and operational logs:** Retained for a limited period necessary for security, debugging, fraud prevention and compliance.

If you need a specific retention commitment for Customer Content, logs, or billing data, please contact us for a DPA or bespoke terms.

9) Security

We implement appropriate **technical and organisational measures**, including: encrypted transport (TLS), encryption at rest by our hosting providers, access controls and least-privilege, environment separation, monitoring and logging, and vendor due diligence. No system is perfectly secure; if we become aware of a **personal data breach**, we will notify affected controllers and/or individuals where required by law.

10) Your rights

Depending on your location (UK/EEA), you may have the right to **access**, **rectify**, **erase**, **restrict** or **object** to processing, and **data portability**, and to **withdraw consent** where consent is the basis.

- **If we process your data as Controller** (e.g., account, payments, support), contact us at **[insert privacy email]** to exercise your rights.
- **If we process your data as Processor** (Customer Content), please direct your request to the applicable **controller** (our customer). We will support them in responding, as required by law and contract.

You also have the right to lodge a complaint with the **Information Commissioner's Office (ICO)** in the UK (see **ico.org.uk**) or your local EEA authority.

11) Cookies

We use **strictly necessary** cookies to operate sign-in, **enable secure payments** (including Stripe's anti-fraud cookies), and keep you logged in. We may use **optional analytics** cookies to understand service usage and improve performance. Where required, we'll obtain your **consent** via a cookie banner and provide controls to withdraw consent at any time. See our Cookie Settings link in the application (if present) for details.

12) Children

The Service is **not intended for children under 13** (or a higher age where required by local law). We do not knowingly collect personal data from children through the Service.

13) AI-generated outputs, accuracy and human oversight

We use **generative AI** to decompose and analyse Customer Content in order to provide fact-checking assistance. **Generative AI can make mistakes.** You remain responsible for reviewing all outputs and for any decisions you make based on them. Outputs are provided for information only and are not legal, medical, financial or other professional advice.

14) Your responsibilities as controller (for business customers)

If you are a business using Brainqub3 Fact Checker:

- You determine the **lawful basis** for processing Customer Content and must ensure any personal data you upload has been collected and shared **lawfully**.
- You must provide **appropriate notices** to data subjects and honour their rights.
- You must not upload content that infringes rights or violates law, and must avoid uploading special category data unless you have a lawful basis and appropriate safeguards.

15) Third-party links

The Service may link to third-party websites or services. Those are governed by their own policies. We are not responsible for their practices.

16) Changes to this policy

We may update this policy to reflect changes to our services or the law. We will post the new version with a new **effective date** and, for material changes, we will notify account owners by email or in-app notice.

17) How to contact us

For questions, requests, or complaints about this policy or our data practices, contact:
DATA-CENTRIC SOLUTIONS LTD (Brainqub3)
86–90 Paul Street, London, England, United Kingdom, EC2A 4NE
Email: **[insert privacy email]**

Annex A – Sub-processors & Key Third Parties (as of the Effective Date)

Provider	Role	Region configured	What they process	Notes
Supabase	Database & Storage	**UK**	Account data (full name, email), Customer Content, operational metadata	Uploaded documents are stored during processing and **deleted after job completion**.
OpenAI	Generative AI inference	*Multiple (may include non-UK/EEA)*	Customer Content and prompts necessary to generate outputs	Processing governed by OpenAI **Data Processing Addendum**: openai.com/policies/data-processing-addendum/

Provider	Role	Region configured	What they process	Notes
Fly.io	Application compute	**London, UK**	Runtime processing of requests, logs necessary for operation	Hosts backend services for the app.
Stripe	**Payments processing & fraud prevention**	*Global (incl. UK/EU/US)*	Payment method details (collected by Stripe), payer identifiers (name, email, billing address), device/technical data for risk, transaction metadata	Stripe may act as **independent controller** for regulated payments/fraud prevention, and processor for certain services. See **stripe.com/privacy**. We do **not** store card numbers or CVC.

Annex B – Summary of processing activities (high-level)

- **Controller activities:** account administration; authentication; **payments via Stripe**; service communications; security monitoring; site operations; optional analytics; legal compliance.
- **Processor activities:** receipt, temporary storage, analysis and transformation of Customer Content to provide fact-checking results; secure deletion of uploaded documents after job completion; assistance with data subject requests and incident response at the controller's instruction.

One-page summary (optional for your website)

- We collect **name and email** to run your account and process payments via **Stripe**.
- Your **uploaded documents are stored in the UK and deleted after the job completes**.
- We use **Supabase (UK)**, **Fly.io (UK region)**, **OpenAI**, and **Stripe** as downstream providers.

- We don’t sell your data; we use it to run and secure the service.
- For rights requests, email **[insert privacy email]** (or contact your organisation if they are the controller).
- Always **review AI-generated outputs**; they can contain errors.