Brainpower Privacy Policy

Effective date: [TO SET ON PUBLICATION] **Last updated:** [TO SET ON PUBLICATION]

---

1. Who we are

Brainpower is a service operated by **UNIO International, Inc.**, a Delaware corporation with its registered office at 131 Continental Dr, Suite 305, Newark, DE 19713, United States ("we", "us", "our").

"Brainpower" and "BRNPWR" are trading names of UNIO International, Inc.

In this policy, "you" means a visitor to brnpwr.com, a person who signs up for an account, or an administrator or billing contact of a business that subscribes to the Brainpower service.

---

2. Scope

This policy covers personal data we handle in connection with:

- The Brainpower website at brnpwr.com;
- The Brainpower account area and dashboard;
- Our sales, onboarding, support, and billing operations.

Two distinct data-protection roles apply to different categories of data:

- **Account and website data - we are Controller.** We decide the purposes and means of processing for the data in this policy. GDPR / UK GDPR / US state privacy laws treat us as controller for that data.
- **Customer workflow content - we are Processor.** When a business customer uses the Brainpower system, the workflow data processed inside the Configured System (learnings, skills configuration, automation patterns, task events, and any text or documents the customer submits) is processed on that customer's instructions. For that data we act as processor under a separate Data Processing Agreement ("DPA") that forms part of the customer's subscription. If you are an end-user on a customer's team, address privacy requests to your employer or directly to your company's Brainpower administrator, not to us.

---

3. Personal data we collect

3.1 Data you provide directly

- **Account data:** full name, work email address, company, hashed password, plan choice.
- **Billing data:** processed by Stripe. We receive the last four digits of your card, card brand, billing country, billing name, and invoice line items. We do not store full card numbers or CVCs.

- **Communications:** messages you send to support, sales, or through forms on the site; meetings you book via Calendly; email correspondence.
- **Referral data:** if you arrive via a referral code, we record the referrer identifier so we can apply the promotion.

3.2 Data collected automatically

- **Technical data:** IP address, browser type and version, device type, operating system, approximate location (city-level inferred from IP).
- **Usage data:** pages viewed, features used, errors encountered, timestamps.
- **Cookies and similar technologies:** essential cookies for authentication and security. Optional analytics and preference cookies are off by default; you opt in through our cookie banner.

3.3 Data we receive from third parties

- **Authentication providers,** if you sign in with Google or a similar provider (name, email, profile identifier).
- **Fraud and abuse signals** from our payment and hosting providers.
- **Publicly available information,** such as LinkedIn profile data used to research prospective customers before outreach.

3.4 What we do not collect

We do not knowingly collect special-category data (health, biometric, racial or ethnic origin, political opinions, religious beliefs, sex life, genetic data) or government identifiers. Please do not submit that kind of information through our systems.

---

4. How we use your data and on what legal basis

Purpose	GDPR / UK GDPR legal basis
Provide and operate the Service	Performance of contract (Art. 6(1)(b))
Authenticate users and secure accounts	Performance of contract + legitimate interest
Process payments and issue invoices	Performance of contract + legal obligation
Respond to support and sales inquiries	Performance of contract / legitimate interest
Send service-related email (security, billing, product changes)	Performance of contract / legitimate interest
Send marketing email to prospects and customers	Consent (opt-in), which you can withdraw at any time
Improve the Service using aggregated, anonymised usage patterns	Legitimate interest
Prevent fraud, abuse, and security incidents	Legitimate interest / legal obligation
Comply with law, tax rules, and legal claims	Legal obligation / legitimate interest

For residents of US states with comprehensive privacy laws (California, Colorado, Connecticut, Virginia, Utah, Texas, and others as laws evolve), these activities align with the statutory bases each state recognises. We do not sell personal information and we do not share it for cross-context behavioural advertising.

---

5. Sub-processors and third-party services

We rely on the following sub-processors to operate the Service. Each is bound by written data-processing terms with appropriate safeguards for international transfers.

Sub-processor	Purpose	Primary location
Anthropic, PBC	Claude AI model inference	United States
Vercel, Inc.	Hosting and serverless execution	United States, with global edge
Notion Labs, Inc.	Database storage for customer profiles, learnings, automation, and events	United States
Stripe, Inc.	Payments, subscription billing, invoicing	United States
Resend, Inc.	Transactional email delivery	United States
Google LLC (Google Workspace)	Email hosting and document productivity	United States
Calendly, LLC	Meeting scheduling	United States

We update this list as sub-processors change. For active customers on a paid subscription, if we add a material new sub-processor we will give at least 14 days' advance notice by email, during which the customer may object on reasonable grounds.

---

6. International data transfers

We are based in the United States. Personal data we collect is processed in the United States and may be accessed from other locations where our staff or sub-processors operate.

Where personal data is transferred from the European Economic Area, the United Kingdom, or Switzerland to the United States or another country, we rely on one or more of the following safeguards:

- The EU-US Data Privacy Framework, where we or the relevant sub-processor is certified and the Framework applies;
- Standard Contractual Clauses issued by the European Commission (Commission Implementing Decision (EU) 2021/914), combined with supplementary technical and organisational measures;
- The UK International Data Transfer Addendum for UK transfers;
- The Swiss-adapted version of the Standard Contractual Clauses for Swiss transfers.

You can request a copy of the safeguards that apply to your data by emailing **privacy@brnpwr.com**.

---

7. EU and UK representative

At our current scale, our processing of EU and UK personal data is occasional and small-scale within the meaning of Article 27(2) GDPR and UK GDPR, so appointment of an EU/UK representative is not

required. We will appoint one and update this policy when thresholds require it.

8. Data retention

Category	Retention period
Active account data	For the life of the account
Closed account data	24 months after closure, for legal, tax, and audit defence
Invoices and billing records	7 years (US tax), or longer where required by applicable local law
Support conversations	36 months after the ticket closes
Marketing consent records	Until you unsubscribe, plus 24 months to evidence prior consent
Server and security logs	12 months
Aggregated, anonymised analytics	Indefinitely (this is no longer personal data)
Customer workflow content (processor role)	Per the subscription term + 60 days, as set in the DPA

9. Your rights

Depending on where you live, you have the following rights. You can exercise any of them by emailing **privacy@brnpwr.com**. We respond within 30 days and may extend once by up to 60 days where necessary, with notice.

- **Access** the personal data we hold about you.
- **Correct** inaccurate or incomplete data.
- **Delete** your data, subject to legal retention requirements.
- **Restrict** or **object to** processing we carry out on the basis of legitimate interest.
- **Portability:** receive your data in a structured, machine-readable format.
- **Withdraw consent** at any time where processing is based on consent.
- **Not be subject to solely automated decisions** that have legal or similarly significant effects (we do not make such decisions).
- **Lodge a complaint** with your local data-protection authority. In the EU/EEA, you can contact your national supervisory authority; in the UK, the Information Commissioner's Office (ico.org.uk).

9.1 California residents (CCPA / CPRA)

In addition to the rights above, California residents have the right to:

- Know what categories of personal information we collect and the purposes;
- Request deletion of personal information;
- Correct inaccurate personal information;
- Opt out of the sale or sharing of personal information (we do not sell or share);
- Limit the use of sensitive personal information (we do not use sensitive personal information for secondary purposes);
- Non-discrimination for exercising these rights.

You may submit requests through **privacy@brnpwr.com**. We verify the request using the email on file. You can designate an authorised agent by providing written authorisation.

9.2 Other US state residents

Residents of Colorado (CPA), Virginia (VCDPA), Connecticut (CTDPA), Utah (UCPA), Texas (TDPSA), and other states with comprehensive privacy laws have equivalent rights to know, delete, correct, and opt out of targeted advertising, sale, and certain profiling. Submit requests via **privacy@brnpwr.com**. We do not engage in targeted advertising, sale of personal information, or profiling with legal or similarly significant effects.

---

10. Security

We maintain technical and organisational measures appropriate to the risk. These include:

- TLS 1.2+ encryption in transit, and encryption at rest for stored personal data;
- Password hashing with modern algorithms;
- Role-based access controls and least-privilege provisioning;
- Multi-factor authentication for staff with production access;
- Logging, monitoring, and documented incident response;
- Regular review of sub-processor security.

No system is perfectly secure. If we become aware of a personal data breach that affects your personal data, we will notify you and relevant regulators without undue delay and within 72 hours where required by law.

---

11. Children

The Service is intended for business use. It is not directed at children, and we do not knowingly collect personal data from anyone under 16. If you believe a child has provided personal data, contact **privacy@brnpwr.com** and we will delete it.

---

12. Changes to this policy

We update this policy when our practices change. Material changes will be announced to account holders by email at least 14 days before they take effect. The current version is always available at brnpwr.com/privacy. The "Last updated" date at the top of this policy reflects the most recent revision.

---

13. Contact us

- **Privacy and data-protection requests:** privacy@brnpwr.com
- **General support:** support@brnpwr.com
- **Legal notices:** legal@brnpwr.com
- **Postal address:** UNIO International, Inc. 131 Continental Dr, Suite 305 Newark, DE 19713 United States