Legal Document

Privacy Policy

This Privacy Policy explains how Another Bright Idea Limited t/a SCAMAdvisory.net collects, uses, stores, protects and discloses personal data when you use our website and services.

WEBSITE	CONTROLLER	TRADING AS	LAST UPDATED
scamadvisory.net	Another Bright Idea Limited	SCAMAdvisory.net	6 April 2026

Important: We do not sell or rent your personal data. We only use and disclose personal data where necessary to operate SCAMAdvisory.net, provide services, process subscriptions, maintain security, comply with legal obligations, and protect our platform and users.

1. Introduction

This Privacy Policy explains how **Another Bright Idea Limited t/a SCAMAdvisory.net** (“we”, “us”, “our”) collects, uses, stores, protects and discloses personal data when you use https://scamadvisory.net, create an account, access our services, view your report history, subscribe to paid services, contact us, or otherwise interact with us.

We are committed to protecting your privacy and handling personal data fairly, lawfully and transparently. We do **not sell or rent** your personal data to third parties.

---

2. Who We Are

Data Controller: Another Bright Idea Limited t/a SCAMAdvisory.net
71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ
Website: https://scamadvisory.net
Privacy contact email: hello@scamadvisory.co.uk

---

3. Scope of This Policy

This policy applies to personal data we process in connection with:

- your website visits;
- your user account;
- login and authentication;
- access to tools, reports and services available through our platform;
- report history and account records;
- subscriptions and billing administration;
- customer support and service communications; and

- security, backup and business continuity operations.

---

4. Personal Data We Collect

Depending on how you use our services, we may collect and process the following categories of personal data.

4.1 Identity and contact data

- name;
- email address;
- telephone number;
- billing or account contact details; and
- any details you provide when contacting us.

4.2 Account data

- username;
- encrypted password and authentication credentials;
- account ID;
- account settings and preferences;
- subscription status; and
- records relating to account creation, login, password resets and account changes.

4.3 Service usage and report history

- records of services you have used;
- report history;
- saved items, activity history and account actions;
- service configuration choices; and
- timestamps linked to your use of the platform.

4.4 Payment and subscription data

Where you purchase a subscription or paid service, we may process:

- subscription plan details;
- billing status;
- transaction reference numbers;
- invoice information; and
- limited payment-related metadata received from our payment provider.

We do not ordinarily store full payment card or bank payment credentials on our own systems where payments are processed by our third-party payment provider.

4.5 Technical and device data

- IP address;
- browser type and version;
- device type;
- operating system;

- session data;
- log files;
- date and time stamps;
- referring pages; and
- other security and diagnostic information.

4.6 Communication data

- emails;
- support tickets;
- contact forms;
- feedback submissions; and
- other correspondence with us.

---

5. How We Collect Personal Data

- directly from you, when you register, subscribe, pay for services, contact us, or use the platform;
- automatically, through your use of the website and services, including technical logs and security monitoring;
- from our payment provider, to confirm payment status, renewals, failed payments or subscription events; and
- from service providers who support hosting, backups, communications or platform operations.

6. How We Use Personal Data

- create and manage user accounts;
- authenticate users and provide secure login access;
- deliver the services and tools available through our platform;
- maintain user report history and service records;
- process subscriptions and administer billing;
- communicate with users about accounts, subscriptions, support and service updates;
- maintain platform security, detect misuse, prevent fraud, and protect the integrity of our systems;
- perform backups, disaster recovery and business continuity operations; and
- comply with legal, tax, accounting and regulatory obligations.

7. Lawful Bases for Processing

Under applicable data protection law, we rely on one or more of the following lawful bases depending on the processing activity.

7.1 Contract

We process personal data where necessary to perform our contract with you, or to take steps at your request before entering into a contract. This includes creating and maintaining your account, providing secure login, giving you access to platform features and services, maintaining account-linked history, managing subscriptions, and providing customer support related to the services you use.

7.2 Legal obligation

We process personal data where necessary to comply with legal obligations, including accounting, tax, fraud-prevention, record-keeping, and lawful disclosure obligations.

7.3 Legitimate interests

We process personal data where necessary for our legitimate interests, provided those interests are not overridden by your rights and freedoms. This includes securing our systems and services, maintaining backups and resilience, investigating abuse, fraud or suspicious activity, administering and improving our services, and keeping appropriate records of service usage, support and operational events.

7.4 Consent

If we use your personal data for any activity that requires consent, such as certain optional marketing or non-essential cookies, we will ask for consent where required by law. You may withdraw consent at any time.

---

8. When Providing Data Is Necessary

Some personal data is necessary for us to provide the service. For example, if you do not provide the information needed to create and verify an account, process a subscription, or authenticate a secure login, we may be unable to provide some or all of the services to you.

---

9. Payments

Subscription and payment services are managed by **GoCardless**. GoCardless processes payment information on its own secure systems in accordance with its own privacy notice, legal obligations, and security controls.

We may receive limited information from GoCardless, such as a customer identifier, subscription status, payment success or failure notifications, renewal dates, billing references, and partial billing information needed for account administration, fraud prevention, record keeping, and customer support.

We use this information to activate services, manage subscriptions, maintain billing records, and respond to payment-related queries.

---

10. Disclosure of Personal Data

We do **not sell or rent** your personal data.

We may disclose personal data only where necessary and proportionate to:

- payment processors that manage subscriptions and billing;
- cloud hosting and infrastructure providers;
- backup, storage and disaster recovery providers;
- communication, email, support or ticketing providers;
- professional advisers, auditors, insurers or legal advisers where needed;
- law enforcement, regulators, courts or public authorities where required by law or to protect legal rights; and
- a purchaser, investor, successor or acquirer in connection with a merger, acquisition, restructuring or sale of assets, subject to appropriate confidentiality safeguards.

Where third-party service providers process personal data on our behalf, we require them to act on our instructions and to implement appropriate security and confidentiality measures.

---

11. International Transfers

Some of our service providers may process or access personal data outside the United Kingdom or European Economic Area. Where this happens, we will take steps to ensure that personal data remains protected in accordance with applicable data protection law.

Where required, we will use an appropriate safeguard, such as an adequacy decision, Standard Contractual Clauses, the UK International Data Transfer Agreement, or another lawful transfer mechanism permitted by applicable law.

If you would like more information about international transfers and the safeguards we use, please contact us.

---

12. Data Security

We take security seriously and use appropriate technical and organisational measures designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

- SSL/TLS encryption for data in transit;
- secure authentication controls;
- access restriction on a need-to-know basis;
- system monitoring and logging;
- regular backups;

- segregation of live and backup environments;
- patching and maintenance procedures; and
- vendor and infrastructure security controls appropriate to the risks involved.

No method of transmission or storage is completely secure, but we work to maintain safeguards proportionate to the sensitivity of the data and the risks presented.

---

13. Backups and Resilience

We perform regular backups for resilience, disaster recovery and business continuity purposes. Backup copies may be stored separately from live systems and retained for a limited rolling period before being overwritten or securely deleted in accordance with our retention practices.

Where backup copies contain personal data, we apply appropriate security controls to those backups.

---

14. Data Retention

We keep personal data only for as long as necessary for the purposes for which it was collected, including to provide services, maintain records, resolve disputes, enforce agreements, and comply with legal and regulatory obligations.

Category	Retention period
Account data	For as long as your account remains active, and for up to 24 months after closure, unless a longer period is needed for legal, security or dispute-resolution

	reasons.
Report history and service records	While your account is active and for up to 24 months after closure, unless you request deletion and we are able to delete sooner.
Support and communication records	Up to 24 months after the last meaningful interaction, unless required for ongoing dispute, complaint or legal reasons.
Technical logs and security records	Normally between 90 days and 12 months, depending on the type of log and the security purpose it serves.
Subscription, billing, invoice and tax-related records	For at least 6 years from the end of the relevant financial year, or longer where required by law or ongoing compliance activity.
Backup copies	Retained on a rolling basis for disaster recovery and then overwritten or securely deleted in line with backup cycles.

You should confirm these periods reflect your actual operational practice before publication.

---

15. Your Rights

Subject to applicable law, you may have the right to:

- request access to the personal data we hold about you;
- request correction of inaccurate or incomplete personal data;

- request erasure of your personal data;
- request restriction of processing;
- object to processing carried out on the basis of legitimate interests;
- request portability of personal data you provided to us, where applicable;
- withdraw consent at any time, where processing is based on consent; and
- complain to a supervisory authority.

To exercise your rights, contact us at hello@scamadvisory.co.uk. We may ask for information to verify your identity before responding.

---

16. Complaints

If you have concerns about how we handle your personal data, please contact us first at hello@scamadvisory.co.uk so we can try to resolve the issue.

You also have the right to lodge a complaint with the relevant supervisory authority. If you are in the United Kingdom, this is the Information Commissioner's Office (ICO).

---

17. Automated Decision-Making

We do not make decisions based solely on automated processing, including profiling, that produce legal effects or similarly significant effects on users, unless we specifically notify you otherwise and have a lawful basis for doing so.

18. Cookies and Similar Technologies

Our website may use cookies or similar technologies for essential functionality, security, session management, and, where applicable, analytics or user experience improvements.

Where legally required, we will request consent before placing non-essential cookies. If you use analytics, advertising, personalisation, or preference cookies, See our Cookie Policy

19. Third-Party Websites and Services

Our website or services may contain links to third-party websites, plugins or services. We are not responsible for the privacy practices of those third parties. We encourage you to review their privacy notices before providing personal data to them.

20. Children

Our services are not intended for children under the age of **18** without appropriate supervision or authority. We do not knowingly collect personal data from children in a manner that requires parental consent unless this is clearly stated.

If you believe a child has provided personal data to us improperly, please contact us and we will review and, where appropriate, delete the information.

21. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in law, regulation, technology, our services, or our processing practices. When we do, we will update the “Last updated” date above.

---

22. Contact Us

Another Bright Idea Limited t/a SCAMAdvisory.net
71-75 Shelton Street, Covent Garden, London, United Kingdom, WC2H 9JQ
Email: hello@scamadvisory.co.uk
Website: https://scamadvisory.net