GaiaScore

ESG Reporting & Sustainability Intelligence Platform

PRIVACY POLICY

Effective Date: 1 January 2025 · Version 1.0 · GaiaScore Ltd

> At GaiaScore, your privacy matters. This Privacy Policy explains what data we collect, why we collect it, how we use it, and your rights over it. We are committed to full transparency and compliance with UK GDPR and the Data Protection Act 2018.

This Privacy Policy applies to all users of the GaiaScore platform — whether you are an Organisation Owner, Admin, Contributor, Consultant, or Viewer. It also applies to visitors to our website at www.gaiascore.com.

Table of Contents

1. Who We Are and How to Contact Us

Data Controller: GaiaScore Ltd

Email: support@gaiascore.com

Website: www.gaiascore.com

GaiaScore Ltd is the data controller responsible for your personal data. If you have any questions about this Privacy Policy or how we handle your data, please contact us at the email above. We aim to respond to all privacy enquiries within 5 business days.

For data protection matters, including Data Subject Access Requests, please email support@gaiascore.com with the subject line **"Data Protection Request"**.

2. What Personal Data We Collect

We collect the following categories of personal data depending on how you use the Platform:

2.1 Account and Identity Data

- Full name and email address (required for registration)
- Profile avatar or photograph (optional)
- Organisation name, industry, size, and location
- Your role within your Organisation (Owner, Admin, Contributor, Consultant, Viewer)
- Google account ID (if you sign in via Google OAuth)

2.2 Usage and Technical Data

- IP address and approximate geographic location
- Browser type, version, and operating system
- Pages visited, features used, and time spent on the Platform
- Login timestamps and session information
- API access logs (Professional Pro and Enterprise plans)
- Error logs and diagnostic information

2.3 ESG and Business Data

- ESG metrics submitted in Assessments (energy, water, waste, people, governance data)
- Sustainability targets, action plans, and progress data
- Materiality assessment responses and stakeholder information
- Advisory chat messages and AI interaction history
- Framework alignment data and badge achievement records
- Evidence files and supporting documentation uploaded to the Platform
- Data Request responses submitted by your team members

2.4 Payment Data

- Billing name and address
- Payment method details (processed and stored by Stripe — GaiaScore does not store card numbers)
- Transaction history and subscription status

2.5 Communications Data

- Support tickets and correspondence with our team
- In-app feedback submitted via the thumbs up/down or feedback features
- Email communications you send to us
- Marketing preferences and communication consent

3. How We Collect Your Data

We collect your data through the following means:

3.1 Directly from you

- When you register for an account
- When you complete an ESG Assessment
- When you set targets, create action plans, or use advisory features
- When you respond to a Data Request
- When you contact our support team
- When you complete onboarding or profile setup

3.2 Automatically

- Usage data collected as you interact with the Platform
- Technical data collected via cookies and similar technologies (see Section 11)
- Log data generated by your use of the API

3.3 From third parties

- Google: name, email, and profile photo when you sign in via Google OAuth
- Stripe: payment and subscription status information
- Your Organisation: when an Owner or Admin invites you and assigns your role

4. Why We Use Your Data — Legal Bases

Under UK GDPR, we must have a lawful basis for processing your personal data. The table below sets out our purposes and the legal basis for each:

Purpose	Data Used	Legal Basis
Provide the Platform and account management	Identity, usage, ESG data	Contract — necessary to deliver the service you signed up for
Process payments and manage subscriptions	Payment and billing data	Contract — necessary to fulfil your subscription
Send transactional emails (verification, password reset, notifications)	Email address, name	Contract — necessary to operate your account
Send Data Request emails to team members	Recipient name and email	Contract / Legitimate Interests
Improve and develop the Platform	Usage and technical data (anonymised)	Legitimate Interests — improving our service for all users
Security monitoring and fraud prevention	IP address, login data, session data	Legitimate Interests — protecting users and the Platform
Comply with legal obligations	Any relevant data	Legal Obligation
Send marketing communications	Email address	Consent — only where you have opted in
Benchmarking and industry research	Aggregated, anonymised ESG data only	Legitimate Interests — advancing ESG reporting standards

5. ESG Data — Special Considerations

> Your ESG data belongs to you. GaiaScore is a tool to help you collect, organise, and report on it. We do not sell your ESG data to third parties, publish it without your consent, or use it to benchmark you against named competitors.

5.1 Data Ownership

All ESG Data submitted to GaiaScore remains the property of your Organisation. GaiaScore holds no ownership claim over your sustainability data, metrics, or reports.

5.2 AI Processing of ESG Data

When you use the AI Advisory feature, your ESG data and organisation context are sent to Anthropic's API to generate responses. This processing is governed by Anthropic's data processing terms. We do not permit Anthropic to use your data to train their models under our current agreement.

5.3 Data Requests

When you send a Data Request to a team member, their name, email address, and submitted ESG data are processed within the Platform. The requesting Organisation is the data controller for this processing. Recipients who are not yet Platform users will receive only the necessary email to complete the request.

5.4 Aggregated Benchmarking

GaiaScore may produce aggregated, anonymised industry benchmarks from ESG data across the Platform. These benchmarks contain no personally identifiable information and no Organisation-specific data. Individual Organisation data is never published without explicit consent.

5.5 Report Sharing

If you enable the shareable report link feature, your ESG report becomes accessible to anyone with the link. You control this setting and can disable it at any time from the Reports section of the Platform.

6. How We Share Your Data

GaiaScore does not sell your personal data. We share data only in the following circumstances:

6.1 Within your Organisation

Members of your Organisation may see your name, role, and activity within the Platform depending on their Role (see Terms of Service, Section 2.4). Owners and Admins can view all member activity. Consultants and Viewers have read-only access.

6.2 Service providers (processors)

We share data with carefully selected third-party processors who help us provide the Platform. All processors are bound by Data Processing Agreements and may only process data on our documented instructions. See Section 7 for the full list.

6.3 Legal requirements

We may disclose your data if required by law, court order, or regulatory authority. We will notify you where permitted before complying with such requests.

6.4 Business transfers

In the event of a merger, acquisition, or sale of GaiaScore Ltd, your data may be transferred to the acquiring entity, subject to equivalent privacy protections. We will notify you before such a transfer takes effect.

6.5 With your consent

We will share your data with other third parties only with your explicit prior consent.

7. Third-Party Services and Integrations

The following third-party services process data on our behalf or in connection with the Platform:

Service	Purpose	Data Shared	Privacy Policy
Stripe	Payment processing and subscription management	Billing name, address, payment method	stripe.com/privacy
Resend	Transactional and notification emails	Email address, name, email content	resend.com/privacy
Anthropic (Claude API)	AI Advisory chat and ESG recommendations	ESG data, organisation context, chat messages	anthropic.com/privacy
Google OAuth	Optional sign-in via Google account	Google account ID, name, email, profile photo	policies.google.com/privacy
Railway / Hosting provider	Platform infrastructure and hosting	All Platform data (encrypted at rest)	railway.app/legal/privacy
PostgreSQL (managed DB)	Data storage	All Platform data (encrypted at rest)	N/A — infrastructure only

We review third-party data processors regularly and update this list when integrations change. We do not currently integrate with analytics platforms (e.g. Google Analytics). GaiaScore products are ad-free — we do not permit advertisers to access your data.

8. International Data Transfers

GaiaScore Ltd is based in the United Kingdom. Your data may be processed or stored by our third-party processors in countries outside the UK, including the United States.

Where data is transferred outside the UK, we ensure appropriate safeguards are in place, including UK International Data Transfer Agreements (IDTAs) or adequacy decisions recognised by the UK Information Commissioner's Office (ICO).

- Stripe processes payment data in the United States — covered by Standard Contractual Clauses.
- Anthropic processes AI data in the United States — covered by Data Processing Agreements.
- Resend processes email data in the United States — covered by Standard Contractual Clauses.

You may request details of our transfer safeguards by contacting support@gaiascore.com.

9. How Long We Keep Your Data

We retain your data only for as long as necessary for the purposes described in this Policy. The following retention periods apply:

Data Type	Retention Period	Reason
Account and identity data	Duration of subscription + 90 days after closure	To allow data export after closure
ESG Assessments and reports	Duration of subscription + 90 days after closure	To allow data export after closure
Advisory chat history	Duration of subscription + 90 days	Capped at 50 messages per conversation
Payment and billing records	7 years from transaction date	UK tax and accounting legal requirement
Support correspondence	3 years from last contact	Legitimate interest — dispute resolution
Usage and technical logs	12 months rolling	Security monitoring and debugging
Marketing consent records	Until consent withdrawn + 3 years	Legal compliance — evidence of consent
Anonymised/aggregated data	Indefinitely	No personal data — used for benchmarking only

After the retention period, data is permanently and securely deleted. Backup copies may persist for up to 30 additional days following scheduled deletion runs.

10. Your Rights Under UK GDPR

You have significant rights over your personal data. We take these rights seriously and will respond to all valid requests within one calendar month.

Right	What it means	How to exercise it
Right of Access	Request a copy of all personal data we hold about you	Email support@gaiascore.com — subject: 'Data Access Request'
Right to Rectification	Correct inaccurate or incomplete personal data	Update in Profile/Settings or email us
Right to Erasure	Request deletion of your personal data ('right to be forgotten')	Email support@gaiascore.com — subject: 'Erasure Request'
Right to Restriction	Ask us to pause processing your data in certain circumstances	Email support@gaiascore.com with details
Right to Data Portability	Receive your data in a machine-readable format	Export from Reports, or request full export via email
Right to Object	Object to processing based on legitimate interests or for marketing	Unsubscribe link in emails, or email us
Rights re: Automated Decisions	Not be subject to solely automated decisions with legal effect	Contact us — our AI features are advisory only
Right to Withdraw Consent	Withdraw consent for marketing at any time	Use unsubscribe link in any marketing email

We will verify your identity before processing requests. We may decline requests that are manifestly unfounded, excessive, or conflict with our legal obligations, but will always explain our reasoning.

There is no charge for exercising your rights, though we may charge a reasonable fee for requests that are manifestly unfounded or excessive.

11. Cookies and Tracking Technologies

11.1 What we use

GaiaScore uses a minimal set of cookies and similar technologies. We do not use advertising cookies, third-party tracking pixels, or behavioural profiling tools.

Cookie / Storage	Purpose	Duration
gs_token (cookie)	Authentication — stores your access token to keep you logged in	Session / 15 minutes
gs_org_id (cookie)	Stores your active Organisation ID for multi-org switching	7 days
gs_user (localStorage)	Caches your user profile (name, email, avatar) for instant display	Until logout
gs_plan (localStorage)	Caches your subscription plan to prevent flash of upgrade screens	Until logout
gs_refresh (localStorage)	Stores refresh token for silent session renewal	30 days
gs_last_org (localStorage)	Remembers your last-used organisation across sessions	Persistent until cleared

11.2 No third-party tracking

GaiaScore does not use Google Analytics, Facebook Pixel, HubSpot tracking, or any third-party behavioural tracking. Your usage of the Platform is not shared with advertisers or data brokers.

11.3 Managing cookies

You can clear browser cookies and localStorage at any time via your browser settings. Clearing authentication cookies will log you out. The Platform does not currently offer a cookie consent banner as we only use strictly necessary cookies and localStorage for Platform functionality.

12. Children's Privacy

The Platform is not directed at or intended for use by children under the age of 16. We do not knowingly collect personal data from children under 16. If you believe a child under 16 has provided us with personal data, please contact us immediately at support@gaiascore.com and we will delete it.

13. Security

GaiaScore takes data security seriously. We implement the following measures to protect your personal data:

- **Encryption in transit:** All data transmitted between your browser and our servers is encrypted using TLS 1.2 or higher.
- **Encryption at rest:** All data stored in our database is encrypted at rest.
- **Access controls:** Role-based access controls limit which team members can see what data.
- **Rate limiting:** API and login endpoints are rate-limited to prevent brute-force attacks.
- **Brute-force protection:** Login attempts are monitored and accounts are protected against credential stuffing.
- **Session management:** Access tokens expire after 15 minutes. Refresh tokens rotate on each use.
- **New login alerts:** You receive an in-app notification and email when a login occurs from a new IP address.
- **Regular reviews:** We conduct periodic security reviews of our infrastructure and code.

Despite these measures, no system is entirely secure. In the event of a data breach that poses a risk to your rights and freedoms, we will notify you and the ICO within 72 hours as required by UK GDPR.

14. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, or legal requirements. When we make material changes, we will:

- Update the Effective Date at the top of this Policy
- Notify registered users by email at least 14 days before changes take effect
- Display an in-app notification for active users

Your continued use of the Platform after the effective date of changes constitutes acceptance of the revised Policy. Previous versions are available upon request.

15. Complaints

15.1 Contact us first

If you have concerns about how we handle your personal data, please contact us first at support@gaiascore.com. We take all privacy concerns seriously and will work to resolve your issue promptly.

15.2 ICO

If you are not satisfied with our response, you have the right to lodge a complaint with the UK Information Commissioner's Office (ICO):

- Website: ico.org.uk
- Helpline: 0303 123 1113
- Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF

You also have the right to seek judicial remedy if you believe your data protection rights have been infringed.

GaiaScore is committed to protecting your privacy and handling your data with care, transparency, and respect.

GaiaScore Ltd · Effective 1 January 2025 · Version 1.0

www.gaiascore.com · support@gaiascore.com