

PRIVACY AND TRACKING POLICY

How We Collect, Use, and Protect Your Information
Including Cookies, Analytics, and Online Tracking Technologies

Effective Date: [June 13, 2026] | Last Updated: [June 13, 2026]

IMPORTANT — READ CAREFULLY: This document is a **sample template** provided for educational and illustrative purposes only. It is **not legal advice** and may not satisfy the specific requirements of GDPR, CCPA/CPRA, ePrivacy Directive, or other applicable privacy, data protection, or consumer protection laws in your jurisdiction or the jurisdictions of your users. Laws change frequently and requirements depend on your exact data processing activities, the types of tracking technologies you actually deploy, whether you "sell" or "share" data, and many other factors. **You must have this policy reviewed, customized, and approved by a qualified attorney** licensed in the relevant jurisdiction(s) before publishing it on your website or relying on it. Using an uncustomized template can expose you to regulatory risk, fines, or lawsuits.

1. Introduction and Scope

CESI-OM LLC ("Company", "we", "us", or "our") operates the website located at <https://cesiusa.com> and any subdomains or related mobile applications (collectively, the "Site"). This Privacy and Tracking Policy ("Policy") describes how we collect, use, disclose, retain, and protect information about visitors, users, and customers of the Site.

This Policy applies to all information collected through the Site, whether you are a visitor, registered user, newsletter subscriber, business partner, or potential investor or customer. It also covers information we collect offline that links to this online Policy.

By accessing or using the Site, you acknowledge that you have read and understood this Policy. If you do not agree with any part of this Policy, please do not use the Site.

2. Categories of Information We Collect

2.1 Information You Provide Directly to Us

We collect personal information that you voluntarily provide when you interact with the Site, including but not limited to:

- Contact or inquiry forms: name, email address, organization/company name, job title, phone number, country, and the content of your message or inquiry.
- Newsletter or update subscriptions: email address, name (optional), and communication preferences (e.g., interest in carbon credit updates, project news, or investor relations).
- Account creation or portal access (if applicable): username, password, profile information, and authentication details.
- Event registrations, webinar sign-ups, or partnership inquiries: relevant professional and contact details.
- Any other information you choose to submit through forms, comments, surveys, or direct communications with us.

2.2 Information Collected Automatically (Tracking & Technical Data)

When you visit or interact with the Site, we and our authorized third-party service providers automatically collect certain technical and usage information. This occurs through server logs, cookies, pixels, scripts, and similar technologies. This data helps us operate the Site securely, analyze performance, detect fraud, and improve the user experience.

Types of automatically collected data include:

- Device and browser information: browser type and version, operating system, device type and model, screen resolution, language settings, and installed fonts or plugins (for device fingerprinting where used).
- Network and location data: IP address (which may reveal approximate city-level geolocation), internet service provider, connection type, and referring/exit URLs.
- Usage and interaction data: pages viewed, time spent on each page, scroll depth, clicks, form interactions, search queries on the Site, navigation paths, and session duration.
- Date, time, and frequency of visits, including repeat vs. new visitors.
- Error logs and performance metrics (page load times, JavaScript errors).

2.3 Information from Third Parties and Public Sources

We may receive or combine information about you from third-party sources, including analytics and advertising partners, social media platforms (if you interact with our content there), public databases, business registries, or data enrichment services. We may also receive information when you interact with our content on third-party sites or when business partners share leads with your consent.

3. How We Use Your Information

We use the information we collect for the following legitimate business purposes:

- **Site Operation & Security:** To provide, maintain, secure, and improve the Site; prevent fraud, abuse, and security incidents; authenticate users; and ensure reliable performance.
- **Analytics & Performance Tracking:** To understand how users navigate and engage with the Site, identify popular content, diagnose technical problems, and make data-driven improvements to design, speed, and functionality.
- **Communication:** To respond to your inquiries, provide customer support, send transactional emails (e.g., form confirmations, password resets), deliver newsletters or project updates you subscribed to, and notify you of important changes to the Site or Policy.
- **Personalization:** To remember your preferences (language, region, cookie choices, display settings) and, where applicable, tailor content or recommendations.
- **Marketing & Business Development:** To promote our [mining / critical minerals / carbon credit / helium / resource project] initiatives, events, or related services (with appropriate consent or legitimate interest where required by law).
- **Legal & Compliance:** To comply with applicable laws, regulations, legal processes, or government requests; enforce our Terms of Service; protect our rights, property, or safety and that of our users or the public; and handle disputes or investigations.
- **Research & Reporting:** To generate aggregated, anonymized, or pseudonymized reports and insights (e.g., for internal planning, investor updates, or demonstrating environmental impact metrics related to avoided emissions or carbon credit generation).

We process personal information only to the extent necessary for these purposes and in accordance with applicable legal bases (consent, legitimate interests, contract performance, or legal obligation).

4. Cookies, Tracking Technologies, and Online Tracking

This section provides detailed information about the tracking technologies we use on the Site. Understanding these technologies is central to this Policy.

4.1 What Are Cookies and Similar Technologies?

Cookies are small text files that are placed on your device (computer, tablet, or mobile) when you visit a website. They are widely used to make websites work more efficiently and to provide information to the site owners. Similar technologies include web beacons (also called tracking pixels or clear GIFs), local storage (HTML5), session storage, device fingerprinting, and server-side logging.

Cookies can be **first-party** (set directly by our Site) or **third-party** (set by our partners, such as Google or advertising networks). They can also be **session cookies** (deleted when you close your browser) or **persistent cookies** (remain on your device for a set period or until deleted).

4.2 Categories of Cookies and Tracking Technologies We Use

A. Strictly Necessary / Essential Cookies

These cookies are required for the Site to function correctly and cannot be disabled through our cookie consent tool. They enable core functionality such as security, session management, load balancing, and accessibility features. Without these cookies, certain parts of the Site may not work properly.

Examples: Session identifiers, CSRF (Cross-Site Request Forgery) protection tokens, load balancer routing cookies, authentication cookies (if login is enabled), and consent preference storage cookies.

B. Performance & Analytics Cookies

These cookies and technologies collect information about how visitors use the Site. They help us measure traffic, understand user behavior, identify popular pages, and improve Site performance and content. Data is typically aggregated and may be anonymized or pseudonymized.

Primary tools we use (or plan to use):

- Google Analytics 4 (or successor) — for page views, sessions, user flows, demographics (aggregated), and event tracking. We [enable / have enabled] IP anonymization where available.
- [Other analytics: e.g., Plausible, Matomo (self-hosted/privacy-friendly), Cloudflare Web Analytics, or Microsoft Clarity — list actual tools]
- Performance monitoring and error tracking (e.g., Sentry or similar).

You can opt out of Google Analytics tracking by installing the official Google Analytics Opt-out Browser Add-on or by adjusting your preferences in our cookie consent banner. Note that aggregated analytics data helps us maintain and improve the Site for all users.

C. Functional / Preference Cookies

These cookies remember choices you make (such as language preference, region, dark/light mode, font size, or cookie consent settings) to provide a more personalized and convenient experience on future visits.

D. Targeting, Advertising & Marketing Cookies / Pixels

These technologies are used to deliver relevant advertisements, measure ad campaign performance, build remarketing audiences, and understand the effectiveness of our marketing efforts across the web. They may track your visit to our Site and other sites you visit.

Current status: We [currently use / do not currently use / plan to use in the future] third-party advertising and remarketing pixels, including but not limited to Google Ads, Meta (Facebook/Instagram) Pixel, LinkedIn Insight Tag, X (Twitter) Pixel, or similar platforms. If we implement these, we will update this Policy and obtain any required consents.

If you are in a jurisdiction that requires opt-in consent for advertising cookies (e.g., many EEA countries), we will only activate these after you have given explicit consent via our cookie banner.

4.3 Other Tracking Technologies

In addition to cookies, we may use:

- **Web beacons / tracking pixels:** Small invisible images embedded in emails or web pages to track opens, clicks, or page views.
- **LocalStorage and SessionStorage:** Browser storage mechanisms used to persist user preferences or session data client-side.
- **Device fingerprinting:** Techniques that combine device attributes (screen size, fonts, plugins, etc.) to create a unique identifier, primarily for fraud prevention, bot detection, or analytics. We [use / do not use] fingerprinting for these purposes.
- **Server-side tracking / Conversions API:** Where supported, we may implement server-to-server tracking to improve data accuracy and privacy (e.g., Meta Conversions API or Google Enhanced Conversions).

4.4 Do Not Track (DNT) and Global Privacy Control (GPC)

Some browsers and browser extensions send a "Do Not Track" (DNT) HTTP header or support the Global Privacy Control (GPC) signal. Because there is currently no uniform, industry-wide standard for how websites should interpret or respond to these signals, our Site **does not currently alter its data collection or tracking practices** in response to DNT or GPC signals. We continue to monitor regulatory and technical developments in this area and may update our practices accordingly.

4.5 Managing Your Cookie and Tracking Preferences

Cookie Consent Banner: On your first visit (and at regular intervals or upon policy changes), we present a cookie consent banner or modal. You can choose to:

- Accept all cookies and tracking technologies
- Reject all non-essential (non-strictly necessary) cookies
- Customize your preferences by category (Analytics, Functional, Targeting, etc.)

Your choices are stored in a cookie (or local storage) so we remember them on future visits from the same browser. You can change your preferences at any time by clicking the "Cookie Settings" or "Privacy Preferences" link usually located in the footer of the Site.

Browser Controls: You can also manage or delete cookies directly through your browser settings. Most modern browsers allow you to block cookies, delete existing cookies, or receive alerts before a cookie is set. Please note that if you disable or delete essential cookies, some features of the Site (such as secure forms, login areas, or personalized preferences) may not function correctly.

Instructions for popular browsers are available on their support sites (search for "manage cookies in [Chrome/Firefox/Safari/Edge]"). Third-party opt-out tools are also available, such as the Network Advertising Initiative (NAI) opt-out page or the Digital Advertising Alliance (DAA) consumer choice tools.

5. Third-Party Services, Embeds, and Links

The Site may integrate or link to third-party services, widgets, embeds, or websites that are not operated by us. These include (but are not limited to):

- Analytics and performance monitoring providers (Google Analytics, etc.)
- Content Delivery Networks (CDNs) and security services (Cloudflare, Fastly, etc.)
- Email marketing and CRM platforms (for newsletters and contact management)
- Social media platforms and embed features (YouTube, X/Twitter, LinkedIn, etc.)
- Mapping or location services (if project sites are displayed)
- Payment processors or investor portal providers (if applicable)
- Document hosting or e-signature services

When you interact with these third-party features, the third party may collect information about you in accordance with their own privacy policies. We encourage you to review the privacy policies of any third-party services you use. We are not responsible for the privacy practices or content of these external sites or services.

6. How We Share and Disclose Information

We do not sell your personal information for monetary consideration in the traditional sense. However, under certain modern privacy laws (particularly the California Consumer Privacy Act / California Privacy Rights Act), the term "sale" or "share" can include disclosures for cross-context behavioral advertising or targeted advertising purposes even without monetary exchange.

We may share information in the following circumstances:

- **Service Providers & Processors:** With trusted vendors, contractors, and subprocessors who perform services on our behalf (hosting, analytics, email delivery, customer support, security). These parties are contractually bound to use the data only for the purposes we specify and to implement appropriate confidentiality and security measures.
- **Legal and Safety:** When required by law, regulation, legal process (subpoena, court order), or governmental request; to enforce our Terms of Service or other agreements; to investigate potential violations; or to protect the rights, property, safety, or security of the Company, our users, or others.
- **Business Transfers:** In connection with a merger, acquisition, corporate reorganization, financing, sale of assets, or bankruptcy. In such cases, we will provide notice if your information becomes subject to a materially different privacy policy.
- **With Your Consent:** When you have explicitly consented to a specific disclosure (e.g., sharing your contact details with a project partner or investor introduction service).
- **Aggregated / Anonymized Data:** We may share aggregated, de-identified, or anonymized data that cannot reasonably be used to identify you for research, marketing, investor reporting, or other legitimate purposes (e.g., total website visitors, aggregated carbon credit interest metrics).

We maintain data processing agreements (DPAs) or equivalent contracts with key service providers as required by GDPR and similar laws.

7. Data Retention

We retain personal information only for as long as necessary to fulfill the purposes for which it was collected, including any legal, accounting, or reporting requirements, unless a longer retention period is required or permitted by applicable law.

Typical retention periods (these are guidelines and may vary):

- Contact form submissions and inquiry records: [24 months] from last interaction, or longer if needed to resolve ongoing matters.
- Newsletter and marketing list subscribers: Until you unsubscribe or request deletion. Unsubscribed emails are retained for a short suppression period to honor your opt-out.
- Analytics and usage data: [14–26 months] for raw event data in tools like Google Analytics (standard configurable retention); aggregated reports may be kept indefinitely.
- Server and security logs: Typically [30–90 days], unless extended for security investigations.

- Legal or compliance records: As required by applicable statutes of limitations or regulatory obligations (often 5–7 years or longer).

When data is no longer needed, we securely delete or anonymize it. You may request earlier deletion of your personal data as described in Section 9, subject to legal exceptions.

8. Data Security

We implement and maintain reasonable and appropriate technical, organizational, and administrative security measures designed to protect your personal information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. These measures include:

- Encryption of data in transit using HTTPS/TLS across the Site.
- Access controls and authentication requirements for internal systems containing personal data.
- Regular security assessments, vulnerability scanning, and monitoring.
- Employee training on data protection and security awareness.
- Use of reputable hosting and infrastructure providers with strong physical and network security.

Despite our efforts, no website, server, or data transmission over the Internet can be guaranteed to be 100% secure. We cannot and do not warrant or guarantee the security of any information you transmit to or from the Site. You transmit information at your own risk. In the unlikely event of a data breach that compromises your personal information, we will notify affected individuals and relevant supervisory authorities as required by applicable law (e.g., within 72 hours under GDPR where feasible).

9. Your Privacy Rights and Choices

Your privacy rights depend on your country or state of residence and the applicable data protection laws. Below is a summary of key rights. To exercise any of these rights, please contact us using the details in Section 13. We will verify your identity before processing certain requests.

9.1 Rights for Individuals in the European Economic Area (EEA), United Kingdom, and Switzerland

If you are located in these regions, you have rights under the GDPR (or UK GDPR) including:

- Right of access — to obtain confirmation and a copy of the personal data we hold about you.
- Right to rectification — to have inaccurate or incomplete data corrected.
- Right to erasure ("right to be forgotten") — to have your personal data deleted in certain circumstances.
- Right to restrict processing — to limit how we use your data in specific situations.
- Right to data portability — to receive your data in a structured, commonly used, machine-readable format and to transmit it to another controller.
- Right to object — to object to processing based on legitimate interests or for direct marketing purposes (including profiling).
- Right to withdraw consent — at any time where we rely on consent as the legal basis (this does not affect processing that occurred before withdrawal).
- Right to lodge a complaint — with your local data protection supervisory authority if you believe we have violated your rights.

9.2 Rights for California Residents (CCPA / CPRA)

If you are a California resident, you have the following rights under the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA):

- Right to Know — what categories and specific pieces of personal information we have collected about you, the categories of sources, the business or commercial purposes for collecting or selling/sharing it, and the categories of third parties with whom we share it.
- Right to Delete — to request deletion of personal information we have collected from you (subject to important exceptions, such as completing a transaction, detecting security incidents, or complying with legal obligations).
- Right to Correct — to request correction of inaccurate personal information.
- Right to Opt-Out of Sale or Sharing — to opt out of any "sale" or "sharing" of your personal information for cross-context behavioral advertising or targeted advertising. [If applicable: You can exercise this right by visiting our "Do Not Sell or Share My Personal Information" link in the footer or by enabling the Global Privacy Control (GPC) signal in your browser.]

- **Right to Limit Use of Sensitive Personal Information** — if we collect sensitive personal information (as defined by CPRA), you may have the right to limit its use to what is necessary to provide the services or as otherwise permitted.
- **Right to Non-Discrimination** — we will not discriminate against you for exercising any of these rights.

Our current practices regarding "sale" or "sharing": We [do not sell or share personal information as defined under the CCPA / CPRA] OR [we engage in limited sharing for targeted advertising purposes as described in Section 4; you may opt out using the mechanisms above]. We will update this section if our practices change.

9.3 Additional Rights and General Controls

- **Marketing Opt-Out:** You may unsubscribe from our newsletters or marketing emails at any time by clicking the "unsubscribe" link in the email or by contacting us directly. We will honor your request promptly.
- **Cookie Preferences:** Manage via our cookie consent tool (footer link) or your browser settings.
- **Account Deletion:** If you have created an account on the Site, you may request deletion of your account and associated data (subject to legal retention requirements).

We aim to respond to verifiable consumer requests within the time periods required by applicable law (typically 30 days, extendable in some cases). If we cannot fulfill a request, we will explain why.

10. International Data Transfers

CESI-OM LLC is based in Tampa, Florida, United States. If you access the Site from outside the United States, your personal information may be transferred to, stored on, and processed by servers or service providers located in the United States or other countries outside your country of residence.

These countries may have data protection and privacy laws that differ from, and in some cases provide less protection than, the laws in your jurisdiction. Where required by applicable law (for example, when transferring personal data from the EEA, UK, or Switzerland), we implement appropriate safeguards to protect your data. These may include:

- Standard Contractual Clauses (SCCs) or the UK International Data Transfer Addendum approved by the relevant authorities.
- Adequacy decisions by the European Commission or UK authorities (where applicable).
- Other approved transfer mechanisms or supplementary measures as needed.

By using the Site, you consent to the transfer of your information to countries outside your country of residence as described in this Policy.

11. Children's Privacy

The Site is not directed to, and we do not knowingly collect personal information from, children under the age of 13 (or under 16 in certain jurisdictions). If you are a parent or guardian and believe that your child has provided us with personal information without your consent, please contact us immediately using the details below. We will take reasonable steps to delete such information from our records as soon as possible.

12. Changes to This Policy

We may update or revise this Privacy and Tracking Policy from time to time to reflect changes in our data practices, the technologies we use, legal requirements, industry standards, or for operational reasons. When we make material changes, we will:

- Update the "Last Updated" date at the top of this Policy.
- Post a prominent notice on the Site (e.g., banner, popup, or dedicated notice page).
- Where required by law or where we have your contact information, notify you by email or other direct means.
- For significant changes that require renewed consent, seek your affirmative consent before applying the new practices.

Your continued use of the Site after the effective date of any updated Policy constitutes your acceptance of the revised terms. We recommend reviewing this Policy periodically.

13. Contact Us

If you have any questions, comments, concerns, or requests regarding this Privacy and Tracking Policy, our data practices, or to exercise your privacy rights, please contact us:

CESI-OM LLC

Attn: Privacy / Data Protection Team
400 North Ashley Drive, Suite 1900
Tampa, FL 33602, United States

Website Contact Form: Please use the contact form available on our website (<https://cesiusa.com>)

Email / Phone: Not provided — inquiries are handled exclusively through the website contact form.

For individuals in the EEA/UK/Switzerland, if we have appointed an EU/UK representative or Data Protection Officer (DPO), their contact details will be provided here or upon request.

Governing Law: This Policy is governed by and construed in accordance with the laws of the State of Florida, United States of America, without regard to its conflict of law principles, except to the extent that mandatory provisions of the data protection or consumer protection laws of your country of residence apply and cannot be overridden by choice of law.

End of Privacy and Tracking Policy Template