

# Privacy & Cookie Policy

Last Updated: March 6, 2026

This Privacy & Cookie Policy explains how EPOCHA ("we," "us," or "our") collects, uses, stores, shares, and protects your personal data, and how we use cookies and similar technologies on our website and through our services. By using our website and services, you consent to the practices described in this policy.

We are committed to protecting your privacy and being transparent about the technologies we use and the data we collect. This policy provides detailed information about our practices and how you can manage your preferences and rights, in compliance with applicable data protection laws, including the General Data Protection Regulation (GDPR) for the European Economic Area (EEA), the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 for the United Kingdom, and the Personal Information Protection Act (PIPA) for South Korea.

## Part 1: Privacy Policy

### 1. Information We Collect

We collect personal data to provide and improve our services to you. This information is collected directly from you when you interact with our website, sign up for services, participate in coaching sessions, or communicate with us, and automatically through your use of our website.

- Personal Identifiable Information (PII): Contact Information: Name, email address, phone number, mailing address.
- Demographic Information: Age, gender, nationality (if relevant for program eligibility, cultural understanding, or legal compliance).
- Academic Information: Educational background, current academic status, university application details, academic goals, and progress within our programs.
- Professional Information: Career aspirations, professional interests.
- Payment Information: Details required for processing payments (e.g., credit card details, bank transfer information). Note: We do not store full credit card numbers; these are processed securely by our third-party payment processor (Stripe/Wise).
- Usage Data (collected automatically): Information about how you access and use our website and services, including your IP address, browser type, operating system, pages viewed, time spent on pages, referring URLs, and device identifiers.
- Details of coaching sessions and device tracking, and engagement with provided materials.
- Communication Data: Records of your communications with us, including emails, chat messages, and call recordings (if applicable and with prior consent).

### 2. How We Use Your Information and Legal Basis for Processing

We use the collected information for various purposes, each with a defined legal basis as required by GDPR/UK GDPR and PIPA:

- To Provide and Manage Services: To deliver coaching sessions, manage your account, process payments, and provide access to resources. Legal Basis: Performance of a contract with you.
- To Personalize Your Experience: To tailor coaching content, recommendations, and support to your individual needs and goals. Legal Basis: Legitimate interests (to improve our services and your satisfaction) or your explicit consent, where required.
- To Improve Our Services: To analyze usage patterns, identify areas for improvement, and develop new programs and features. Legal Basis: Legitimate interests (to enhance our offerings and user experience).
- For Communication: To send you important updates, service-related announcements, and administrative messages. Legal Basis: Performance of a contract (for service-related communications) or legitimate interests (for important updates).
- To send you newsletters and promotional materials about our services. Legal Basis: Your explicit consent (for direct marketing) or legitimate interests (for existing customers, with an easy opt-out).
- For Security and Fraud Prevention: To protect our website and services from unauthorized access, fraud, and other illegal activities. Legal Basis: Legitimate interests (to ensure the security and integrity of our services) and compliance with legal obligations.
- For Legal Compliance: To comply with applicable laws, regulations, and legal processes (e.g., tax obligations, data protection requests). Legal Basis: Compliance with a legal obligation.

### 3. How We Share Your Information and International Data Transfers

We do not sell or rent your personal data to third parties. We may share your information with:

- Service Providers: Trusted third-party vendors who perform services on our behalf, such as payment processing (Stripe/Wise), email delivery, analytics (Google Analytics), and platform hosting (Zoom, Teams, Canva). These providers are contractually obligated to protect your data and use it only for the purposes for which we disclose it to them, in accordance with our instructions and applicable data protection laws. Legal Requirements: When required by law, court order, or governmental regulation, or if we believe it's necessary to protect our rights, property, or safety, or the rights, property, or safety of others.
- Business Transfers: In the event of a merger, acquisition, or sale of all or a portion of our assets, your personal data may be transferred as part of the transaction. We will notify you via email or a prominent notice on our website of any such change in ownership or control of your personal data. With Your Consent: We may share your information with third parties when we have your explicit consent to do so.
- International Data Transfers: As an international service, your personal data may be transferred to, stored, and processed in countries outside of your country of residence, including the UK, EEA, and South Korea, where data protection laws may differ.

For EEA/UK Users: When we transfer your personal data outside the EEA or UK, we ensure a similar degree of protection is afforded to it by implementing at least one of the following safeguards:

- Transferring personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission or UK government.
- Using specific contracts approved by the European Commission or UK government which give personal data the same protection it has in the EEA/UK (Standard Contractual Clauses - SCCs).
- Where we use providers based in the US, we may transfer data to them if they are part of the Data Privacy Framework (if applicable) or if we have implemented SCCs.

For South Korean Users: When transferring personal data overseas, we will obtain your explicit consent or ensure that the transfer falls under a legal exception as per PIPA. We will inform you of the recipients, the purpose of transfer, the items of personal information to be transferred, and the retention period of the personal information.

### 4. Data Retention and Destruction (South Korea PIPA Specific)

We retain your personal data only for as long as necessary to fulfill the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

For South Korean Users (PIPA): When personal information becomes unnecessary due to the expiration of the retention period, achievement of the purpose of processing, or termination of the service, we will destroy it without delay.

Destruction Procedure: Personal information stored in electronic file formats will be deleted using technical methods that prevent restoration. Personal information recorded on paper will be shredded or incinerated.

### 5. Data Security

We implement appropriate technical and organizational measures to protect your personal data from unauthorized access, alteration, disclosure, or destruction. These measures include:

- Encryption of data in transit and at rest where appropriate.
- Access controls and authentication procedures for our systems.
- Regular security assessments and vulnerability testing.
- Employee training on data protection and security best practices.
- Incident response plans to address potential data breaches promptly.

However, please be aware that no method of transmission over the internet or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your personal data, we cannot guarantee its absolute security.

### 6. Your Data Protection Rights

Depending on your location and applicable data protection laws (e.g., GDPR, UK GDPR, PIPA), you may have the following rights regarding your personal data:

- Right to Access: Request a copy of the personal data we hold about you.
- Right to Rectification: Request correction of inaccurate or incomplete personal data.
- Right to Erasure ("Right to be Forgotten"): Request deletion of your personal data under certain conditions.
- Right to Restrict Processing: Request restriction of processing your personal data under certain conditions.
- Right to Data Portability: Request transfer of your data to another organization or directly to you, under certain conditions.
- Right to Object: Object to the processing of your personal data under certain conditions, including processing for direct marketing.
- Right to Withdraw Consent: Where we rely on your consent to process your personal data, you have the right to withdraw that consent at any time. This will not affect the lawfulness of any processing carried out before you withdraw your consent.
- Right to Lodge a Complaint: You have the right to lodge a complaint with a supervisory authority if you believe your data protection rights have been violated.

For UK Users: Information Commissioner's Office (ICO).

For EEA Users: Your local Data Protection Authority (DPA).

For South Korean Users: Korea Internet & Security Agency (KISA) or the Personal Information Protection Commission (PIPC).

To exercise any of these rights, please contact us using the details provided in the "Contact Us" section below. We will respond to your request in accordance with applicable data protection laws.

### 7. Personal Information Protection Officer (PIPO) / Data Protection Contact

For any inquiries or concerns regarding your personal information and data protection, please contact our designated data protection [contact](#).

## Part 2: Cookie Policy

This section explains how Student Ascent uses cookies and similar technologies on our website.

### 1. What are Cookies?

Cookies are small text files that are placed on your computer or mobile device when you visit a website. They are widely used to make websites work more efficiently, as well as to provide information to the owners of the site. Cookies allow a website to "remember" your actions or preferences over time.

We also use other similar technologies, such as web beacons, pixel tags, and local storage, to collect information about your browsing activities and preferences. For simplicity, we will refer to all these technologies as "cookies" in this policy.

### 2. How We Use Cookies

We use cookies for various purposes, including:

- Strictly Necessary Cookies: These cookies are essential for the operation of our website. They enable core functionalities like security, network management, and accessibility. Without these cookies, our website cannot function properly. They do not store any personally identifiable information. (Legal Basis: Legitimate Interests - necessary for website functionality)
- Performance and Analytics Cookies: These cookies collect information about how you use our website, such as which pages you visit most often, and if you experience any errors. This helps us understand and analyze user behavior, improve the performance of our website, and enhance your user experience. We may use third-party analytics services (e.g., Google Analytics) for this purpose. (Legal Basis: Your explicit consent)
- Functionality Cookies: These cookies allow our website to remember choices you make (such as your username, language, or the region you are in) and provide enhanced, more personalized features. They can also be used to remember changes you have made to text size, fonts, and other parts of web pages that you can customize. (Legal Basis: Your explicit consent)
- Targeting and Advertising Cookies: These cookies are used to deliver advertisements more relevant to you and your interests. They are also used to limit the number of times you see an advertisement and help measure the effectiveness of advertising campaigns. They are usually placed by advertising networks with our permission. They remember that you have visited a website and this information may be shared with other organizations, such as advertisers. (Legal Basis: Your explicit consent)
- Social Media Cookies: These cookies are set by a range of social media services that we have added to the site to enable you to share our content with your friends and networks. They are capable of tracking your browser across other sites and building up a profile of your interests. This may impact the content and messages you see on other websites you visit. (Legal Basis: Your explicit consent)

### 3. Types of Cookies We Use

- First-Party Cookies: These are cookies set by the website you are visiting (i.e., by KIIAC).
- Third-Party Cookies: These are cookies set by a domain other than that of the website you are visiting. For example, when you use our website, we may integrate services from third parties like Stripe and Wise (for payments). These third-party services may set their own cookies to enable their features and track their performance. We do not control these third-party cookies.
- Session Cookies: These cookies are temporary and expire when you close your browser. They are used to link your actions during a single browsing session.
- Persistent Cookies: These cookies remain on your device for a set period of time specified in the cookie, or until you delete them. They are used to remember your preferences or actions across multiple visits.

### 4. Your Choices and Managing Cookies

You have the right to decide whether to accept or reject cookies. For non-essential cookies, we will obtain your explicit consent through a cookie banner or consent management platform upon your first visit to our website.

You can also exercise your cookie preferences by adjusting your browser settings. Most web browsers allow some control of most cookies through the browser settings.

Please note that if you choose to disable cookies, some parts of our website or services may not function properly or may become inaccessible.

Here's how you can manage cookies in common browsers:

Google Chrome:

- Go to Settings > Privacy and security > Site Settings > Cookies and site data.
- You can block all cookies, block third-party cookies, or clear cookies when you close Chrome.

Mozilla Firefox:

- Go to Options > Privacy & Security > Cookies and Site Data.
- You can choose to block third-party cookies, manage data, or clear data.

Apple Safari:

- Go to Safari > Preferences > Privacy.
- You can select "Prevent cross-site tracking" and "Block all cookies."

Microsoft Edge:

- Go to Settings > Privacy, search, and services > Tracking prevention.
- You can choose your tracking prevention level and block third-party cookies.

For specific third-party cookies, you may have additional opt-out options:

- Google Analytics: To prevent your data from being used by Google Analytics, you can install the Google Analytics opt-out browser add-on.

## Part 3: General Information

### 1. Changes to This Privacy & Cookie Policy

We may update this Privacy & Cookie Policy from time to time to reflect changes in our practices or for other operational, legal, or regulatory reasons. We encourage you to review this policy periodically to stay informed about how we are protecting your information. Any changes will be effective immediately upon posting the updated policy on our website.

### 2. Contact Us

If you have any questions or concerns about our Privacy & Cookie Policy, our data practices, or your rights, please [contact](#) us.