Privacy Policy for Avenirs

Effective Date: 04 July 2025

At Avenirs, your privacy is a priority. This Privacy Policy explains how we collect, use, share, and protect your data in compliance with the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other applicable laws.

1. Data We Collect

We collect personal and usage data that enables us to deliver personalized services and continuously improve the user experience:

- **Personal Data:** This includes information provided during registration or while using the platform: full name, email address, age, gender (optional), school name, current grade level, geographic location, favorite school subjects, preferred learning styles, career goals, language proficiency, and future study or work plans. These data points are essential for tailoring education and career recommendations.
- **Usage Data:** We collect behavioural and technical data, including pages visited, features used, click behaviour, login times, time spent on the platform, session duration, and referral sources. These analytics help us evaluate and improve the user experience.
- **Device and Browser Information:** Automatically collected metadata such as IP address, browser type and version, device type, operating system, and screen resolution. This data helps us optimise the platform for your device and ensure platform security.

2. How and Why, We Use Your Data

We process personal data for specific, legitimate purposes under GDPR Article 5(1)(b):

- **Personalization of Services:** To generate custom recommendations on educational paths and career options based on user profile data.
- **Platform Optimization:** To monitor performance, resolve bugs, and develop new features based on aggregated user behavior.
- **Security and Compliance:** To identify suspicious activity, prevent fraud, and comply with legal and regulatory obligations.
- **User Communication:** To send essential information related to account activity, service updates, technical notices, and, if opted in, newsletters or promotional messages.

Each processing activity is carried out under a lawful basis as explained in the GDPR Compliance Statement section.

3. Data for Minors

- We collect and process data of users aged under 18 through a mandatory consent checkbox during registration. At this step, the user is presented with the full Privacy Policy and Terms and Conditions. Consent is given by checking the box stating: "I understand and agree to Avenirs processing my data as described in the Privacy Policy and Terms and Conditions." The IP address, timestamp, and content of the consent interaction are

logged and stored securely for verification purposes. This approach ensures compliance while maintaining a smooth onboarding process for minors.
- We do not intentionally collect sensitive personal data ("special categories of data") as defined in GDPR Article 9, such as racial or ethnic origin, political opinions, religious beliefs, or health-related data. Users are advised not to submit such information.

4. Data Sharing and Third Parties

- **We do not sell or rent personal data to anyone.**
- We may share anonymized or aggregated data with educational research institutions or policy partners to improve guidance outcomes and contribute to education-related studies.
- We use vetted third-party vendors (e.g., cloud service providers, analytics platforms) to support core operations. These providers act as **data processors** under GDPR Article 28 and are contractually bound to handle data securely and only as instructed.
- We perform due diligence and ensure Data Processing Agreements (DPAs) are in place before engaging any external vendor.

5. Data Security

We take appropriate technical and organizational measures to ensure data protection as required under GDPR Article 32:

- **Encryption:** All data is encrypted during transmission (TLS/HTTPS) and at rest (AES-256 or equivalent).
- **Access Controls:** Only authorized personnel with a clear need-to-know can access personal data.
- **Monitoring:** We conduct regular system audits, vulnerability scans, and have automated alerting in place for suspicious activity.

6. Your Rights (GDPR-Compliant)

As a data subject, you have the following rights under GDPR:

- **Right of Access (Article 15):** You can request a copy of the personal data we hold about you.
- **Right to Rectification (Article 16):** You can ask us to correct inaccurate or incomplete data.
- **Right to Erasure (Article 17):** Also known as the "right to be forgotten," you may request deletion of your data.
- **Right to Restrict Processing (Article 18):** You can ask us to stop processing your data under certain conditions.
- **Right to Data Portability (Article 20):** You may request your data in a commonly used, machine-readable format.
- **Right to Withdraw Consent (Article 7):** If our processing is based on consent, you may withdraw it at any time.
- **Right to Lodge a Complaint (Article 77):** You may file a complaint with your national Data Protection Authority if you believe we've mishandled your data.

To exercise these rights, please contact us at: info@avenirs.co. We respond to requests within 30 days, as per GDPR requirements.

7. Retention Policy

- We retain user data only for as long as necessary to fulfil the purposes outlined above or to meet legal obligations.
- Account and profile data may be retained for up to 24 months following the last recorded login. After this period, data will be anonymised or permanently deleted unless the user reactivates their account or requests continued storage.
- Backups are encrypted and retained for security and disaster recovery purposes but are purged regularly in compliance with our retention schedule.