SCOLINGO PRIVACY POLICY

Scolingo is a global platform that respects your privacy and is committed to protecting your personal data in accordance with applicable data protection laws. This Privacy Policy is aligned with the General Data Protection Regulation (EU) 2016/679 (GDPR), as well as relevant national laws, including the Law on Personal Data Protection of the Republic of Serbia.

This document explains what types of personal data we collect from users and how, why, and in what way such data are processed. It also describes how long we store data, under what circumstances we share them with third parties, what protection measures we apply, and what rights you have concerning your data and how you can exercise them.

This Privacy Policy applies to all users of the Scolingo platform, including students, tutors, and administrators, regardless of the country from which they access our service. All users are guaranteed the same level of protection of their personal data, whether they are located in Serbia, the European Union, or elsewhere, in accordance with the above-mentioned regulations.

By accessing or using the Scolingo platform, you acknowledge that you have read and agreed to the provisions of this Privacy Policy. If you do not agree with any provision of this Policy, please discontinue use of the platform.

Note: This Privacy Policy applies solely to the Scolingo platform and its services. Our platform may contain links to external websites or services of third parties over which we have no control. We recommend that you review the privacy policies of each such third-party website or service you visit, as Scolingo is not responsible for how those third parties handle your data

1. Identity of the Data Controller

The data controller is the Scolingo platform (hereinafter: "Scolingo" or "we").

Contact details of the controller: For any questions regarding the protection of personal data, you may contact us via email at: **contact@scolingo.com**

2. Types of Data Collected

Scolingo collects various types of data from users depending on how the platform is used. Categories of personal data we may collect include:

- **Data provided directly by the user:** Information you personally enter during registration or use of the platform. This includes identifying and contact information such as full name, email address, phone number, place of birth, place of residence, username and password (unless using external login), and other information you voluntarily provide. For example, users may enter additional profile data (such as photo, profile description, interests, or qualifications), information about their educational status or institution (if applicable), etc. We may also collect content you upload or

generate using the platform—e.g. assignments, classroom messages, comments, ratings, and feedback—to the extent such content may contain personal data.

- **Technical (automatically collected) data:** When using the Scolingo platform, our system automatically collects certain data about your device and access method for the functioning and security of the service. These data may include, for example: the IP address of the device you access from, browser type and version, device operating system and platform, unique device or cookie identifiers, date and time of access, pages visited on the platform, session duration, actions you perform, and similar usage logs. These technical data help ensure proper service operation, tailor platform display to your device, and help us understand and analyze how users engage with the platform (see section on cookies and analytics).

- **Data obtained from third parties:** In certain cases, we collect personal data indirectly, through external services or partners you use within the platform:
    - *Authentication via Google account:* If you register or sign in to Scolingo using Google Login, we receive certain information from your Google profile with your permission. This typically includes your first and last name, email address, and optionally your profile photo associated with the Google account. We use this data solely for creating and managing your Scolingo account. (Note: When authenticating through Google, Google's privacy policy also applies; we recommend that you review it.)
    - *Payment processing via Stripe:* Scolingo uses the Stripe service for secure payment processing (see section 6 for more details). When you make a payment on the platform, certain data about you and the transaction are forwarded to Stripe (such as your name, billing address, transaction amount, and card details). Stripe may return limited transaction information (e.g. confirmation of payment, transaction ID, card type, etc.), which we record for payment tracking and delivery of paid services.
    - *Analytics and other data:* We may use tools for analytics or integrate with third-party services (e.g. email notification services, analytics tools such as Google Analytics) that collect certain information about the user and activity on the platform. Data generated by such tools (e.g. usage statistics, aggregated demographic data) may be available to Scolingo but are typically anonymous or pseudonymized. If we receive any of your personal data through such tools, we will use them only for the purposes outlined in this Policy and in compliance with data protection laws.

Note: Scolingo does not collect or process special categories of personal data ("sensitive data"), such as information on racial or ethnic origin, political opinions, religious beliefs, health status, or biometric data, unless strictly necessary to provide a specific service and with appropriate consent or legal basis. The platform is not intended for users to publish such sensitive data, and we ask that you refrain from entering them into platform content.

3. Purposes and Legal Bases for Processing

Your personal data is collected and processed solely for clearly defined purposes and on appropriate legal bases, in accordance with GDPR and applicable data protection laws. The primary purposes include:

- **Provision and operation of platform services:** To allow you to use the Scolingo platform and its functionalities, we process your data when creating and maintaining user accounts, enabling access to lessons, courses or content, connecting students and

tutors, and supporting communication and interaction within the platform. This includes identity verification during login (via email or Google) and saving your preferences or settings.

- **Payment processing and financial records:** When purchasing services, subscriptions, or other paid content on the platform, we process necessary data to complete those transactions, confirm payments, and maintain financial records. This involves working with our payment service provider (Stripe) and storing relevant transaction information.

- **Customer support and communication:** We use your contact information and communication content to respond to your inquiries, support requests, or complaints, and to send you service-related notices. This includes, for example, emails regarding changes to the Terms of Use or Privacy Policy, notifications about scheduled lessons, system messages (e.g. for email verification, payment confirmation, password reset), and similar.

- **Sending informational and marketing communications:** With your prior consent, we may occasionally use your contact details (e.g. email) to send newsletters, announcements about new features, special offers, educational materials, or other promotional communications related to Scolingo and associated services.

- **Service analysis and improvement:** We use usage data (including technical and aggregated data) to understand user behavior and needs, assess the effectiveness of our educational programs, and develop or improve platform functionalities. This may include internal usage reports, tracking popular courses or features, limited testing of new functions, collecting user feedback, and more. Wherever possible, we use anonymized or pseudonymized data for these purposes (i.e. without directly identifying you).

- **Security and abuse prevention:** We process your data to protect the legality and integrity of our platform and its users. This includes fraud detection, threat monitoring, unauthorized access prevention, identity verification to prevent impersonation, violation detection (e.g. prohibited content), and investigation and response to incidents (e.g. unusual account activity). We may also retain data to protect our legal interests in the event of disputes (e.g. keeping evidence).

- **Compliance with legal obligations:** We may process your data as required to fulfill our legal obligations under applicable laws. This may involve using or storing data for compliance with accounting or tax regulations, data protection laws, or disclosure to competent authorities (e.g. in judicial, administrative, or regulatory proceedings, upon lawful request or court order).

4. Data Retention Policy

Personal data is retained in a format that allows identification only for as long as necessary to fulfill the purposes for which they were collected and processed, unless longer retention is required or permitted by law. The retention period depends on the type of data and its processing purpose:

- **User account data:** Core user information (e.g. name, contact, profile) and associated content are retained as long as you maintain an active account. If you delete your account (or request deletion), we will remove or anonymize your personal data within a reasonable timeframe, except where retention is required due to legal obligations or legitimate interests (e.g. evidence of consent, proof of dispute resolution). If your account remains inactive for a prolonged period, we reserve the right to remove it from active systems after prior notification, to minimize storage of unnecessary data.

- **Payment and transaction data:** Payment records and financial transaction data are stored as required under applicable accounting and tax laws. Typically, this means retaining such records for at least 5 years—and potentially up to 10 years—after the close of the fiscal year in which the transaction occurred, or longer if required by audit rules or regulatory authorities. After expiration, data is securely deleted or anonymized unless still needed for ongoing legal matters.
- **Technical and log data:** System access logs, event logs, and other technical records collected automatically during use of the platform are retained as long as reasonably necessary for their intended purpose. For example, security-related logs are generally retained for several months up to one year. Aggregated, non-identifying analytics data may be retained longer for statistical purposes. If needed for security incident investigation or legal compliance, logs may be retained until no longer required, and then deleted or anonymized.
- **User support communication:** Communications with support (e.g. email messages, requests and responses) and related documentation are retained as long as necessary to address your inquiry or complaint, and for a subsequent period (usually up to 2 years) to maintain records in case of follow-up or dispute. If such records are relevant for protecting our legal rights (e.g. in court), they may be retained until the matter is resolved or the statutory limitation expires.

After the above periods, personal data will be permanently deleted or irreversibly anonymized (rendered unidentifiable).

Important: Even after deletion from active databases, some data may remain temporarily stored in secure system backups. Scolingo maintains backup cycles to protect against data loss; all personal data in backups is also subject to deletion or overwrite within a short retention window. If the system is restored from backup, we will ensure that any deletion requests received in the meantime are respected.

5. User Rights Concerning Data

In accordance with applicable data protection laws (GDPR and local regulations), individuals whose personal data is processed (data subjects) have the following rights, which Scolingo respects:

- **Right of access:** You have the right to obtain confirmation from us whether we process your personal data, and if so, to access those data. You may request a copy of all your personal data we hold, as well as details about how and why we process them (e.g. processing purposes, categories of data, data recipients, retention periods, etc.).
- **Right to rectification:** You have the right to request correction or completion of your personal data if they are inaccurate, outdated, or incomplete. For example, if you change your email address or discover an error, you may ask us to update that information. (Note: many of your basic data can be updated via your account settings.)
- **Right to erasure:** In certain circumstances, you have the right to request deletion of your personal data. For example, this applies if the data are no longer necessary for the purposes for which they were collected, if you withdraw consent, if you object to processing based on legitimate interest, or if data is being processed unlawfully. Please note that this right is not absolute—we may refuse erasure to the extent that continued processing is necessary (e.g. to comply with legal obligations or participate in legal proceedings). You will be informed of the basis for any such retention.
- **Right to restriction of processing:** You may request temporary restriction of data processing in specific cases, such as if you contest the accuracy of the data (for the time

needed to verify it), or if processing is unlawful but you prefer restriction instead of deletion, or if we no longer need the data but you need them for legal claims. While restricted, we will retain your data but not otherwise process them without your consent or legal justification. You will be informed in advance if the restriction is lifted.

- **Right to data portability:** You have the right to receive your personal data, which you previously provided to us, in a structured, commonly used, and machine-readable format, and to transmit them to another controller of your choice, if technically feasible. This applies to data processed by automated means and based on your consent or contract. Upon request, we may transfer data directly to another provider, if feasible.
- **Right to object:** You have the right to object at any time to the processing of your personal data. In particular, you always have the right to object to processing for direct marketing purposes (including profiling related to such marketing). If you object to such processing, your data will no longer be used for that purpose. If you object to processing based on legitimate interest, we will cease processing unless we demonstrate compelling legal grounds that override your interests, rights and freedoms, or the data are needed for legal proceedings.
- **Right to withdraw consent:** Where data is processed based on your consent, you may withdraw that consent at any time. Withdrawal applies to future processing only—it does not affect lawfulness of processing carried out before withdrawal. For example, if you consented to receiving newsletters, you may unsubscribe at any time (e.g. via a link at the bottom of the email). For other matters, contact us using the details in Section 11.
- **Right not to be subject to automated decisions:** You have the right not to be subject to a decision based solely on automated processing (including profiling) which produces legal effects concerning you or similarly significantly affects you. In such cases, you have the right to request human review, express your views, and contest the decision.
  Note: Scolingo does not currently use your data for automated decision-making with legal or similarly significant effects (e.g. fully automated assessments affecting educational success). If we introduce such systems in the future, we will notify you and ensure that all legal safeguards are provided.
- **Right to lodge a complaint with a supervisory authority:** If you believe your data rights have been violated or data is processed unlawfully, you have the right to file a complaint with the relevant data protection authority. In Serbia, this is the Commissioner for Information of Public Importance and Personal Data Protection. In EU countries, you may contact the data protection authority in your country of residence or where the violation occurred. We encourage you to contact us first to resolve any issue, but your right to lodge a complaint remains unaffected.

To exercise any of the above rights, please contact us using the details in Section 11 of this Policy (e.g. by sending a request via email). We may need to verify your identity before fulfilling the request (e.g. to ensure we do not disclose your data to another person). We will respond without undue delay, and no later than 30 days from receiving the request, unless the complexity or volume of the request requires an extension, in which case you will be informed.

6. Use of Data Processors and Disclosure to Third Parties

Scolingo cooperates with trusted third parties—partners and service providers—in the provision of its services, to whom it may be necessary to grant access to certain personal data of users. These third parties generally act as data processors on behalf of Scolingo, meaning they process the data exclusively under our instructions and for our purposes, in compliance with this Privacy Policy and with appropriate data protection agreements. In certain cases, some

partners may act as independent controllers for specific data you provide them (for example, a payment service provider may be required to retain your transaction data for their own regulatory purposes). Below are the main categories and examples of third parties with whom we share data, and the reasons for such sharing:

- **Payment Service Providers (Stripe):** To process payments and financial transactions on the platform, we rely on Stripe, a reputable online payment service. When you make a payment via credit/debit card on the Scolingo platform, the payment data (card number, expiration date, CVC code, transaction amount, your name and billing address, etc.) is entered directly through the Stripe integration. This data is sent directly to Stripe, which processes it in accordance with its own privacy policy and strict industry security standards (PCI DSS). Scolingo does not store sensitive financial information such as your card number or security code on its servers. Stripe only shares essential information with us regarding the transaction—such as transaction ID, payment status (success or failure), card type (Visa, Mastercard, etc.), the last four digits of your card, and so on—so that we can register the payment, grant access to paid content, and maintain financial records. We have entered into a Data Processing Agreement with Stripe, ensuring that Stripe will process users' personal data solely for the purpose of executing payments and in compliance with the GDPR. More information about how Stripe handles data is available in their Privacy Policy.
- **Authentication Providers (Google):** As previously mentioned, Scolingo allows users to register and log in using their Google account, via Google Sign-In/Out. In this context, Scolingo exchanges data with Google: when you choose to sign in with Google, you will be redirected to Google's platform where you enter your Google credentials (email/password or use an already active session). With your consent, Google then shares your basic information with us—typically your name, surname, and the email address associated with your Google account (and possibly the URL of your profile photo, if you approve it). Scolingo uses this data to (a) verify your identity and successfully log you into the platform and (b) create a user account linked to your Google email if it's your first time. Google may collect additional information about your use of our platform in connection with this authentication (e.g., that you signed into Scolingo), but such data is subject to Google's terms of use and privacy policy. Scolingo does not share any additional personal data with Google beyond what is necessary for authentication (e.g., login token). Once logged in, Google does not process your data on our behalf. It is important to understand that your relationship with Google is separate from Scolingo; if you have questions about how Google uses your data, we recommend reviewing their privacy policies.
- **Hosting Providers and Infrastructure:** The Scolingo platform is built using modern technologies and third-party infrastructure. This means your data may be stored and processed on servers provided by specialized hosting or cloud service providers (e.g., data centers, cloud platforms). These technical providers may locate their servers in multiple countries (including outside Serbia or the EU), but are contractually obligated to ensure data confidentiality and appropriate protection standards.
- **Other External Contractors:** From time to time, Scolingo may engage additional parties to support our operations, such as email or SMS service providers (for verification codes, notifications, etc.), providers of analytics and usage tracking tools (like Google Analytics or other platforms), IT system maintenance partners, or external consultants and auditors (e.g., legal, security, or financial advisers). In each such case, we share only the minimum amount of personal data necessary for the performance of that specific service. For example, our email service receives your email address and message content for delivery; analytics tools may collect anonymized or

pseudonymized data on your usage; an IT partner may temporarily access the database to resolve a technical issue, etc. All such parties are contractually bound (either through data processing agreements or confidentiality clauses) to use your data solely for authorized purposes, to keep it secure and confidential, and to return or delete it once no longer needed.

Scolingo does not sell or rent your personal data to any marketing agencies or unauthorized third parties. All third-party data access occurs either based on your choices or for the fulfillment of requested services (as in the case of payment), or for internal needs (such as hosting and analytics). At all times, we retain control over how and for what purposes our partners may process your data.

We may also disclose certain personal data to third parties outside the aforementioned processors in the following specific circumstances:

- if required by law or competent authorities, in good faith belief that such disclosure is reasonably necessary (e.g., responding to a subpoena, court or regulatory order, legal process, or statutory obligation);
- if necessary to protect our rights, property, or safety, or the rights and safety of our users or other individuals (this may include sharing information with law enforcement);
- in the event of a corporate transaction such as a merger, acquisition, restructuring, or asset sale involving Scolingo, your data may be transferred to the new owner or partner, with the obligation to continue using it in accordance with this Privacy Policy. In any such change, we will aim to notify you before a change in the data controller occurs.

7. International Data Transfers

Given that Scolingo operates globally and uses infrastructure and services of partners located in various countries, your personal data may be transferred to and stored outside the country in which you reside or outside the country in which the data were originally collected. This includes transfers of data outside the European Union/European Economic Area (EU/EEA) or outside the Republic of Serbia. For example, our primary servers may be located in one country, while backup servers or services we use (such as Stripe or Google) may be located in other countries (including the United States of America).

In any case, we will endeavor to transparently inform you about where your data are stored and processed. If you have any questions regarding the transfer of your data to other countries, please contact us (see Contact Information). Upon your request, we may provide you with additional information regarding the safeguards we have implemented for international data transfers, as well as copies of relevant contractual clauses.

Note: By using the Scolingo platform, you understand that your data may be transferred to and processed outside your home country. However, this does not affect your rights – Scolingo ensures that, regardless of where the data are processed, appropriate safeguards apply in accordance with this Policy and applicable laws.

8. Technical and Organizational Data Protection Measures

Scolingo applies high standards of information security in order to protect users' personal data from unauthorized access, disclosure, alteration, or destruction. We have implemented

appropriate technical and organizational measures for the protection of personal data. These measures include, among others:

- **Encryption of data:** All data exchanged between users and our platform via the website or application are transmitted through secure protocols. This means that information (e.g., data entered during registration or login, payment data, etc.) is protected against interception while transmitted over the Internet. Where applicable, sensitive data are encrypted at rest (on disk).
- **Account and password security:** User passwords are stored on our servers in hashed form (one-way cryptographically processed), which provides additional protection – neither employees nor third parties can view your original password. The system is designed so that even in the unlikely event of unauthorized access to the database, your password remains unknown. We also provide two-factor authentication options where available and limit the number of failed login attempts to prevent brute-force attacks.
- **Access control and confidentiality:** Internally, access to users' personal data is restricted to authorized members of the Scolingo team who require such data to perform their duties (the "need-to-know" principle). All employees and engaged associates who may come into contact with personal data are bound by confidentiality agreements and have undergone training regarding data protection rules. We have defined procedures for managing user access, so that access rights are granted, modified, and revoked in accordance with job responsibilities and termination of necessity.
- **Firewall, antivirus and monitoring:** Our IT infrastructure is protected by modern firewall systems that filter unauthorized access, as well as antivirus/anti-malware solutions that detect and prevent malicious activities. We regularly monitor system logs in order to detect suspicious activity and use intrusion detection systems where possible. Through automated tools, we can be alerted in case of unusual activity patterns that may indicate a security issue.
- **Updates and maintenance:** Our software systems, servers, and applications are regularly updated with patches and security upgrades as soon as they become available, in order to reduce the risk of exploiting known vulnerabilities. Security checks and testing (including internal testing and, occasionally, external penetration testing engagements) are regularly conducted to identify and eliminate potential system weaknesses.
- **Pseudonymization and data minimization:** Wherever feasible, we apply pseudonymization techniques – replacing your personal identifiers (such as name) with artificial identifiers – where it is not necessary for data to be directly attributable to you during processing. We also collect only those data that are necessary for specific, clearly defined purposes (data minimization principle), avoiding excessive data collection. For example, if your phone number or residential address is not required for a specific service, we will not request it.
- **Recovery plan and backup:** We have established procedures for regular data backups and disaster recovery plans in order to ensure business continuity and data integrity even in the event of unforeseen circumstances (such as serious hardware failure, incident, or natural disaster). Backup copies are stored in encrypted form and at separate locations, with strictly controlled access.
- **Privacy by design:** When developing new functionalities or services, Scolingo applies the principles of "privacy by design and by default." This means that data protection is taken into account already at the software planning stage – we use privacy-friendly default settings (e.g., private profiles, reasonable visibility limitations), while users may optionally choose to share more data if they wish. Each new data processing activity is

subject to internal compliance assessment (and, in the case of high risk to users' rights, to a formal Data Protection Impact Assessment – DPIA, in accordance with GDPR).

Although we strive to apply all economically reasonable and organizationally appropriate protective measures, it is important to emphasize that no data transmission over the Internet or data storage system is 100% secure. Therefore, we cannot guarantee absolute security of information in all circumstances. However, Scolingo continuously monitors developments in information security standards and adapts its measures to maintain a high level of protection.

In the unlikely event of a personal data breach that may jeopardize your privacy, Scolingo is obligated to act in accordance with legal requirements. This includes notifying the competent supervisory authority within the legally prescribed timeframe, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Furthermore, if we determine that a breach may result in a high risk to your rights and interests, we will inform you without undue delay, in accordance with the law, together with information on measures taken to mitigate potential harm. You may always contact our team if you suspect any compromise of your data.

9. Cookie Policy (Cookies)

Like most modern online platforms, Scolingo uses cookies and similar technologies in providing its services. Cookies are small text files placed by our website on a user's device (computer, tablet, phone) when you visit our page, serving various purposes such as ensuring basic website functionality, remembering your preferences, or collecting statistical data. Below we describe which types of cookies we use and why.

Categories of cookies used by Scolingo:

- **Essential cookies:** These cookies are crucial for the functioning of the platform and enable you to use basic features. For example, essential cookies allow you to remain logged in during a session without repeatedly entering credentials on each page (session cookies), remember data entered into forms while navigating the site, or assist in server load balancing. Without these cookies, certain parts of the platform would not function properly. Essential cookies are generally first-party cookies (set by us), and the data collected through them are not used for promotional purposes.
- **Functional cookies:** These cookies are not strictly necessary but significantly enhance your user experience. They remember your choices and settings to display the platform in a manner tailored to your preferences. This way, you do not have to reselect settings each time you visit. These cookies may be set by us or by third parties whose services we have integrated into the platform (e.g., a video player or chat module placing its own functional cookie).
- **Analytical cookies:** These cookies help us understand how users use our platform, enabling us to improve it. Through analytical cookies, we collect anonymized or aggregated data regarding page visits, time spent on specific sections, interaction with features, source of traffic (e.g., search or direct access), etc. For this purpose, we may use third-party cookies that collect information about your use of the site and generate statistical reports (e.g., total number and demographics of visitors, popularity of content). These data do not identify individual users but serve to identify general trends. We use analytical information internally to improve content quality and user experience.
- **Marketing cookies:** Currently, we do not use marketing cookies or advertising network cookies on the Scolingo platform. This means that no cookies are collected through our

websites for targeted advertising purposes by third parties, nor do we share your data with advertising partners for remarketing campaigns. All cookies we use serve exclusively the functional or analytical purposes described above, related to improving our own service. If Scolingo decides in the future to use cookies for marketing purposes, we will do so in accordance with the law, with your prior consent and explicit identification of such cookies in an updated Policy.

Cookie management: Upon your first visit to our platform, in accordance with applicable regulations, you will be presented with a notice regarding the use of cookies. For cookies that are not essential (such as analytical cookies), we will request your consent before placing them on your device. You may change your cookie preferences at any time: you may delete existing cookies or block acceptance of new cookies through your browser settings. However, please note that disabling certain categories of cookies (especially essential ones) may affect platform functionality – for example, you may not be able to remain logged in or certain features may not function properly.

For more information on how we use cookies or how you can manage their settings, you may consult our separate Cookie Policy (if available on the website) or contact us. By continuing to use our platform without changing your browser cookie settings, you are deemed to have consented to our use of cookies as described herein.

10. Processing of Data of Minors

The protection of children's and minor users' privacy is of particular importance to us. The Scolingo platform is not intended for children under the age of 14, and we do not knowingly collect personal data from individuals of that age without verified consent from a parent or legal guardian. We request that children under 14 do not use or attempt to register on the platform independently. If we discover that we have collected information about a child under 14 without parental consent, we will take steps to delete such data from our records as soon as possible.

For minor users of older age (above 14 but below the legal age for independent consent), the platform may be available only under the supervision and with the consent of a parent or legal guardian. Minors under the age of 18 cannot independently provide valid consent for data processing in the context of information society services (online platforms), although countries may prescribe a lower age subject to a minimum threshold.

If you are a parent or guardian and have any concerns regarding your child's data on our platform, we encourage you to contact us (see Section 11 – Contact). Upon your request, we may provide access to your child's data, correct inaccurate data, or delete the child's profile (except to the extent we are required to retain it).

If we learn that we are processing the data of a minor without appropriate parental/guardian consent (where such consent is legally required), we will immediately suspend further processing of such data. We will take steps to remove such data from our systems unless the parent/guardian approves continued processing.

Please note that this policy regarding minors applies globally – for users in different jurisdictions we will apply the stricter of two standards (e.g., if local law prescribes a different age for consent, we will act accordingly, but in no case below the age of 14). Our goal is always

to ensure a safe and appropriate environment for young users, in cooperation with parents, schools, and guardians.

11. Contact Information and Amendments to the Policy

Contact for data protection:
If you have any questions, requests, or complaints regarding this Privacy Policy or the processing of your personal data on the Scolingo platform, please contact us. The fastest way is via email at: **contact@scolingo.com**.

We will endeavor to respond to all inquiries as soon as possible, and no later than within the statutory deadlines. If you are exercising any of the rights listed in Section 5 or reporting an issue, please provide sufficient information in your message so that we can understand and process your request effectively (e.g., the email address associated with the account concerned, description of the issue, etc.).

Amendments to the Privacy Policy:
Scolingo reserves the right to amend or supplement this Privacy Policy from time to time, in accordance with changes in our business operations or legal obligations. When we update the Policy, we will revise the date of the latest revision indicated at the bottom of the document. Each new version shall enter into force upon publication on our website/platform, unless otherwise provided.

In the case of material changes that significantly affect your rights or the manner in which we use your personal data, we will make reasonable efforts to notify you directly in an appropriate manner. This may include sending a notification via email to the address associated with your account or displaying a notice within the platform upon login. In this way, you will be able to review the amended Policy and decide whether you wish to continue using the service under the new terms.

We recommend that you periodically review this Privacy Policy in order to stay informed about any changes. If you continue to use the Scolingo platform after amendments to the Privacy Policy have entered into force, it shall be deemed that you accept the amended data processing terms. Naturally, if you do not agree with the amendments, you have the right at any time to request deletion of your account and discontinue use of the service

This Privacy Policy shall enter into force on February 11, 2026, and shall remain valid until amended or withdrawn in accordance with the Terms of Use.

Version 1.0