EdBot

Privacy Policy

How we handle your information, in plain terms and in full legal detail

Version 1.0
Last updated: 19 October 2026
Effective date: 19 October 2026

Controller: EdBot LLC, Albania
Contact: edbotsupp@gmail.com

Contents

Privacy at a Glance . . . 3
1. Introduction and Scope . . . 4
2. Who We Are and How to Contact Us . . . 5
3. How EdBot Is Built: Our Local-First Approach . . . 6
4. Information We Collect . . . 8
5. Information We Do Not Collect or Store . . . 10
6. How We Use Information . . . 11
7. Legal Bases for Processing . . . 12
8. AI Processing and AI Providers . . . 13
9. Uploads, Documents, Images and the Homework Scanner . . . 15
10. Storage on Your Device . . . 15
11. Sharing and Disclosure . . . 16
12. International Data Transfers . . . 18
13. Cookies, Local Storage and Similar Technologies . . . 19
14. Analytics and Product Measurement . . . 20
15. Payments and Subscriptions . . . 20
16. Children and Teens . . . 21
17. Schools, Course Centres and Institutional Plans . . . 23
18. Data Retention . . . 24
19. Data Security . . . 25
20. Your Rights and How to Exercise Them . . . 26
21. Regional Supplements . . . 28
22. Automated Decision-Making and Profiling . . . 31
23. Safety, Abuse Prevention and Content Moderation . . . 32
24. Marketing Communications . . . 33
25. Research, Pilots and Feedback . . . 33
26. Features Under Development . . . 33
27. Third-Party Links and Services . . . 34
28. Changes to This Policy . . . 34
29. Contact, Complaints and Supervisory Authorities . . . 34
30. Glossary . . . 35
Appendix A: Data Inventory . . . 36
Appendix B: Service Providers and Sub-processors . . . 36
Appendix C: Template for Making a Privacy Request . . . 37
Appendix D: Summary of the Legal Framework . . . 37
Appendix E: Cookies and Local Storage Items . . . 38

Privacy at a Glance

This page is a short, plain-language summary. It is **not** a substitute for the full policy that follows, which is the legally binding document. If anything here seems to differ from the full text, the full text applies.

The short version

Your study material stays on your device. Conversations, uploads, notes, saved material and progress are kept in a local database file on your own device. EdBot does not keep a central archive of your schoolwork.

We hold very little. Beyond a minimal account (for example your email address and plan), we store nothing about what you study or ask.

AI requests pass through us, but are not stored by us. When you ask a question, your request is relayed through our server to an AI model provider and the answer is returned. Nothing is written to disk or kept on EdBot infrastructure. The AI provider receives the request in order to answer it and may keep it briefly under its own terms (see Section 8).

We do not sell your data and we do not run ads. We do not use your content to build advertising profiles, and we do not use your content to train AI models.

Local storage has trade-offs. If you clear your browser data, lose your device or reset it, your material may be gone, and we cannot recover it. Use the export feature to make your own backups (Section 10).

Young users are protected. EdBot is designed for secondary-school and university students. There are age rules and parental involvement requirements (Section 16).

You have rights. You can ask us to access, correct, delete or export your account data, object to certain uses, withdraw consent and complain to a regulator (Section 20). Contact: edbotsupp@gmail.com.

Question	Short answer	Where to read more
Where is my study material kept?	In a local database file on your device.	Sections 3 and 10
What does EdBot store on its servers?	Minimal account, subscription and technical data. No content.	Sections 4, 5 and 18
Who sees my questions?	The AI provider that generates the answer, in transit and briefly on its side. Not EdBot staff.	Sections 8 and 11
Is my data sold or used for ads?	No.	Sections 6 and 11
Is my data used to train AI models?	Not by EdBot, and our providers are configured not to train on it.	Section 8
Can children use EdBot?	Minimum age applies; parental permission is needed below certain ages.	Section 16
How do I delete everything?	Delete local data in the app and request account deletion.	Sections 10 and 20
Who do I contact?	edbotsupp@gmail.com or your national regulator.	Sections 2 and 29

1. Introduction and Scope

1.1 Purpose of this policy

EdBot is an educational platform that takes a student from a difficult question to understanding, practice and saved study material. It combines an AI tutor, document and image uploads, a homework scanner, explanation modes, learning paths, a quiz and exam engine and a progress dashboard. Because students may be minors, may upload identifiable assignments and may type personal things into a chat box, we take the protection of personal data seriously and have designed EdBot to hold as little of it as possible.

This Privacy Policy explains what personal data EdBot collects, where it is kept, why we process it, who we share it with, how long we keep it, how we protect it and what rights and choices you have. It is written to meet the transparency obligations of the laws that apply to us, principally the Albanian Law no. 124/2024 "On the Protection of Personal Data" and, because EdBot is offered internationally, the EU General Data Protection Regulation (GDPR) and other national laws described in Section 21.

1.2 Who this policy applies to

This policy applies to every person whose personal data we process in connection with EdBot, including:

- **Visitors** to our website and landing pages who have not created an account;
- **Registered users** on the free plan, the Premium plan or any trial or beta programme (including closed beta participants);
- **Parents and guardians** who create, pay for, supervise or give permission for a younger user's account;
- **Teachers, course-centre staff and institutional administrators** who use EdBot under an institutional plan (see Section 17);
- **Pilot and research participants** who take part in interviews, surveys or structured pilots (see Section 25);
- **Newsletter subscribers, referral invitees and people who contact us** by email, forms or social media; and
- **Individuals whose information appears in material a user uploads**, for example a classmate named in a document or a teacher's name on a worksheet (see Section 9).

1.3 What this policy covers

This policy covers the EdBot website, the EdBot web application (including when it is used from a phone browser or installed as a web app), the server-side relay that connects the application to AI model providers, our support and feedback channels, our marketing communications and any other service that links to this policy (together, the "**Service**").

1.4 What this policy does not cover

- Third-party websites, apps and services that EdBot may link to or that you may use alongside EdBot (for example your school's learning platform, a search engine or a social network). Their own privacy policies apply.

- Processing that an educational institution carries out for its own purposes. Where a school or course centre decides why and how student data is processed, the institution is responsible for that processing and for its own privacy notice (Section 17).
- Information you keep on your own device outside EdBot's control, such as screenshots or files you saved separately.

1.5 How this document is organised

The policy is arranged in layers. "Privacy at a Glance" gives the short version. Sections 2 to 20 are the core policy that applies to everyone. Section 21 contains regional supplements for people in particular jurisdictions. Sections 22 to 30 cover specific topics and administrative matters. The appendices contain a detailed data inventory, a list of service providers, a guide to making requests and a summary of the legal framework.

1.6 Language and versions

EdBot is English-first and multilingual. This policy is published in English and will be made available in Albanian. Translations are provided for convenience. Where a translation and the English text differ, the English text prevails except where mandatory local consumer law requires otherwise. Earlier versions of this policy are available on request and are listed in Section 28.

1.7 Defined terms

"**Personal data**" means any information relating to an identified or identifiable natural person. "**Processing**" means any operation performed on personal data, such as collecting, storing, using, transmitting or deleting it. "**Controller**" means the party that decides why and how personal data is processed. "**Processor**" means a party that processes personal data on behalf of a controller. Other terms are explained in the Glossary in Section 30.

2. Who We Are and How to Contact Us

2.1 The data controller

For the personal data described in this policy, the controller is the entity operating EdBot:

Item	Details
Controller	EdBot LLC
Country of establishment	Albania
Privacy contact (all requests and questions)	edbotsupp@gmail.com

2.2 Data protection contact or officer

We have designated the EdBot privacy team as responsible for data protection, reachable at edbotsupp@gmail.com. Where the law requires us to appoint a Data Protection Officer, that person will be named here and notified to the competent authority. You may contact this person about any question concerning this policy or about the exercise of your rights.

2.3 Representatives in other jurisdictions

Because EdBot is established in Albania and offers its Service to people in other countries, some laws require us to appoint a local representative, for example under Article 27 of the GDPR for the European Economic Area and Article 27 of the UK GDPR for the United Kingdom. Where such a requirement applies to us, we appoint a representative and publish their details in this section. Until then, you can always reach us directly at edbotsupp@gmail.com, and we will pass your request on to the competent authority or representative where the law requires it.

2.4 When we act as a processor

Where an educational institution purchases EdBot for its students under an institutional plan and determines the purposes and means of the processing of its students' data, EdBot may act as a **processor** on the institution's behalf. In that case we process the data only on the institution's documented instructions under a data processing agreement, and the institution is the controller responsible for informing its students and for responding to their requests (Section 17).

2.5 How we handle questions about this policy

If you have a question that this policy does not answer, write to us. We aim to reply within **five working days** and to resolve rights requests within the deadlines set out in Section 20. If you are a young person, you are welcome to ask a parent, guardian or teacher to contact us on your behalf.

3. How EdBot Is Built: Our Local-First Approach

Most of what makes EdBot different from other study tools is a design decision about where information lives. Understanding it makes the rest of this policy easier to follow.

3.1 The design principle

Students may be minors, and the material they work with is personal: homework, exam preparation, notes, mistakes. The safest way to protect information is not to hold it. EdBot is therefore built so that **there is as little to protect as possible**. Beyond the minimum account data, EdBot does not store your study material. Uploads, conversations, notes, saved material and progress live in a local database file on your own device.

3.2 The three zones

Zone	What is there	Who can access it	Retention
1. Your device	Conversations, uploaded documents and images, scanner results, notes, flashcards and quizzes you create, study plans, progress and scores, interface preferences.	You, and anyone who can use your device or browser profile. Not EdBot.	Until you delete it, clear your browser or app data, or lose the device.
2. The relay (in transit)	Each request you send to the AI tutor, including any text, document excerpt or image included in it, and the answer returned.	Processed automatically in memory by our server and by the AI provider that generates the answer.	Not written to disk or retained by EdBot. The AI provider may retain it briefly under its terms (Section 8).

Zone	What is there	Who can access it	Retention
3. EdBot records	Minimal account data, subscription status, usage counters, technical and security logs, analytics events that contain no content, support correspondence.	A small number of authorised EdBot personnel and our service providers.	As set out in Section 18.

3.3 Why the relay exists

AI model providers require credentials (API keys). If those credentials were placed in your browser, anyone could extract and abuse them. We therefore pass your requests through our own server, which holds the credentials securely, attaches them, forwards the request to the chosen model and returns the result. The relay also applies usage limits, performs abuse checks and routes each request to the model best suited to its complexity. The relay is designed to be a pass-through: **nothing is written to disk or retained on EdBot infrastructure**.

3.4 What “pass through without being stored” means precisely

We want to be accurate rather than reassuring, so we explain the limits of this statement:

- While a request is being processed, it necessarily exists in the memory of our server for the fraction of a second to a few minutes it takes to complete. That is processing, even though nothing is stored afterwards.
- Our hosting infrastructure records technical metadata about requests (for example time, size, status and network address) in operational logs. These logs do **not** contain the text of your questions, your uploads or the answers.
- The AI provider that generates the answer receives your request. We do not control the provider’s systems. Its handling is governed by our agreement with it and by the provider’s own terms, which may allow short-term retention for safety and abuse monitoring (Section 8).
- If an error occurs, our error reports are configured to exclude request content.

3.5 What this means for you

- **Privacy benefits:** there is no central archive of student work that could be breached, subpoenaed, mined or misused. EdBot staff cannot read your study material.
- **Control:** you can delete your local data yourself, without waiting for us.
- **Limitations:** we cannot restore lost local data, cannot sync it across devices unless a future feature says so, and cannot help you recover a conversation or note that is no longer on your device. We also cannot look into a particular answer you received, because we do not keep it.
- **Responsibility:** the security of the local database depends in part on the security of your device (Section 10).

4. Information We Collect

This section lists the categories of personal data we process, where each comes from, and what it includes. A consolidated table appears in Appendix A.

4.1 Account and profile information

When you register, we collect the minimum needed to operate your account:

Data	Why it is needed	Notes
Email address	To create and secure your account, send service messages and let you recover access.	Required unless you sign in with a supported third-party identity provider.
Display name or nickname	To personalise the interface.	Optional. We recommend not using your full legal name.
Authentication data	To verify it is you who is signing in.	Passwords are stored only as salted hashes. If you use a third-party login, we receive an identifier and the email address you authorise.
Age confirmation or age band	To apply age-based protections (Section 16).	We ask for an age band or an age confirmation rather than your full date of birth.
Country or region and language	To apply the right legal terms, pricing and language.	May be inferred from your browser settings and network address.
Plan and account status	To apply the correct limits and features.	Free, Premium or institutional.

4.2 Subscription and payment information

If you buy Premium, our payment provider collects your payment details directly. We receive confirmation of the transaction, the plan and billing period, the amount and currency, a customer or subscription reference, the country, tax information needed for invoicing and the last four digits and type of the card, where provided. **We do not receive or store full card numbers.** See Section 15.

4.3 Usage counters and limits

To enforce the daily limits of the free plan and the fair-use limits of Premium, we count how many requests, uploads and other limited actions are associated with your account or device in a period. These counters contain numbers and timestamps, not the content of your requests.

4.4 Technical and device information

When you use the Service, our servers and hosting infrastructure automatically receive information such as your network (IP) address, browser type and version, operating system, device type, screen size, language setting, time zone, the pages or functions you call, the date, time and result of each request, referring website and crash or error diagnostics. We use it to deliver the Service, keep it secure, detect abuse and diagnose faults.

4.5 Product analytics events

To understand whether EdBot is helping students, we record limited events about how the product is used, such as “a question was asked”, “material was saved”, “a practice set was started” and “a session ended”. These events are linked to a pseudonymous identifier. **They do not contain what you asked, uploaded or wrote.** Section 14 explains how these events are used and your choices.

4.6 Communications

If you contact us, respond to a survey, report a problem or give feedback, we keep what you send us, including your email address, the content of your message, any attachment you choose to include and our replies. Please do not include sensitive information or other people’s data in messages to us unless it is necessary.

4.7 Newsletter, referrals and community activity

If you subscribe to updates, we process your email address and your subscription preferences. If you use a referral link or invitation, we process the referral code and, to credit a referral, a record that a new account was created through it. If you interact with us on social media or student communities, we see what you publicly post to us and the platform’s own identifiers.

4.8 Pilot and research participants

If you take part in a pilot, interview or survey, we collect the information you provide, such as your age range, school level, study habits, opinions and, where you agree, a recording or notes of an interview. Participation is voluntary and is explained in a separate information sheet (Section 25).

4.9 Information from other sources

- **Identity providers:** if you choose to sign in with a third-party account, we receive the information you authorise that provider to share.
- **Payment providers:** transaction status, subscription status, refunds, chargebacks and fraud signals.
- **Parents and institutions:** if a parent, guardian, teacher or institution creates or manages an account for you, they provide your name or email address and the plan.
- **Security and fraud-prevention sources:** reputation information about network addresses or devices used to attack online services.

4.10 Study content that you create or upload

Your questions, documents, photos, notes, flashcards, quizzes, exam attempts, study plans and progress are created and kept on your device. When you ask the AI tutor or another AI-powered feature to work with them, the relevant content is sent through the relay for processing as described in Sections 3 and 8. We do not hold a copy.

4.11 Sensitive information

We do not ask you for sensitive categories of personal data, such as health information, religious or philosophical beliefs, ethnic origin, political opinions, sexual orientation, biometric identifiers or information about criminal convictions. However, study content can include such information incidentally: for example a biology problem about a genetic condition, a history essay about a political movement, or a message in which a student describes how they feel. Where this happens, the content is handled in the same way as all other content: it stays on your device and passes through the relay without being stored. We do not use such content to build profiles or to infer sensitive characteristics about you.

5. Information We Do Not Collect or Store

Being clear about what we do not do is as important as saying what we do. In the ordinary use of the Service, EdBot:

- **does not store** your questions, conversations, uploaded documents, photos, notes, flashcards, quiz or exam answers, study plans or progress on EdBot servers;
- **does not maintain** a central archive or searchable database of student work;
- **does not collect** precise location, contacts, calendar, photo library or files other than those you deliberately upload;
- **does not access** your microphone or camera except when you use a feature that requires it, such as the homework scanner or, in future, voice, and only after you grant permission through your browser or operating system;
- **does not create** voiceprints, facial templates or other biometric identifiers, and does not use facial recognition or emotion recognition;
- **does not use** advertising identifiers, third-party advertising cookies or cross-site tracking;
- **does not sell** personal data, and does not “share” it for cross-context behavioural advertising;
- **does not use** your content to train, fine-tune or improve AI models, and has configured its providers accordingly (Section 8); and
- **does not build** profiles of individual students for sale to schools, employers, universities, insurers or any other third party.

> **A note on promises**
>
> No system can honestly promise perfect privacy or perfect security. The statements above describe how EdBot is designed and operated today. If we ever need to change them, we will update this policy, tell you in advance where the change is material and, where the law requires, ask for your consent before the change applies to you.

6. How We Use Information

We use personal data only for specified, explicit and legitimate purposes, and not in ways that are incompatible with them. The table below sets out each purpose, the data used and the legal basis relied on (explained in Section 7).

Purpose	Data used	Legal basis
Create and manage your account; authenticate you	Account data, authentication data, technical data	Contract (Art. 6(1)(b) GDPR and equivalent)
Provide the Service: relay your requests to AI models and return answers; apply limits	Request content in transit only; usage counters; account status	Contract
Process payments, issue invoices, handle refunds and subscriptions	Subscription and payment data; account data	Contract; legal obligation (tax and accounting)
Keep the Service secure; prevent fraud, abuse and automated misuse; enforce limits and terms	Technical data, usage counters, account data, abuse signals	Legitimate interests; legal obligation where applicable
Diagnose faults and maintain performance	Technical data, error diagnostics	Legitimate interests
Measure whether the product works (activation, loop completion, return visits) and improve it	Pseudonymous analytics events without content	Consent where required by law (e.g. ePrivacy rules); otherwise legitimate interests
Communicate service messages (security alerts, receipts, changes to terms or policy)	Email address, account data	Contract; legitimate interests
Respond to enquiries, requests and complaints; provide support	Communications data, account data	Contract; legitimate interests
Send newsletters and product updates; run referrals	Email address, preferences, referral data	Consent (and legitimate interests for existing customers where permitted)
Run pilots, interviews and surveys	Participant data	Consent
Comply with legal obligations; respond to lawful requests; establish, exercise or defend legal claims	Any data we hold that is necessary	Legal obligation; legitimate interests
Protect a child or another person from serious harm	Data strictly necessary in the circumstances	Vital interests; legal obligation
Plan and complete corporate transactions (e.g. financing, merger)	Data we hold, to the minimum extent needed	Legitimate interests

6.1 What we will not do

- We will not sell personal data or use it to serve third-party advertising.
- We will not use personal data in a manner incompatible with the purposes above without informing you and, where required, obtaining consent.
- We will not make decisions that have legal or similarly significant effects on you solely by automated means (Section 22).
- We will not combine data from your study content with other data to create profiles, because we do not hold your study content.

6.2 Purpose limitation and compatible use

If we want to use personal data for a new purpose, we first assess whether it is compatible with the original purpose, taking account of the link between the purposes, the context in which the data was collected, its nature, the possible consequences for you and the safeguards in place. If it is not compatible, we will seek your consent or find another lawful basis, and we will update this policy.

6.3 Aggregated and anonymised information

We may create statistics that cannot reasonably be used to identify any individual, for example "the percentage of new users who complete the question-to-practice loop in their first session". We may use and share such information (including with prospective education partners and funders) because it is not personal data. We will not attempt to re-identify it and will contractually prohibit recipients from doing so.

7. Legal Bases for Processing

Data protection laws require a lawful basis for each processing activity. We rely on the following bases. Where a different law uses different terminology, we apply the closest equivalent.

7.1 Performance of a contract

We process account, subscription and relay data because it is necessary to provide the Service you have asked for under our Terms of Service, or to take steps at your request before entering into it. If you do not provide the minimum account data, we cannot create your account.

7.2 Consent

Where we rely on consent (for example for non-essential analytics, marketing emails, optional features such as voice, or participation in a pilot), the consent is freely given, specific, informed and unambiguous, and given by a clear affirmative action. You may withdraw it at any time through the settings in the app, the link in any email or by contacting us. Withdrawal does not affect the lawfulness of processing before withdrawal. Withdrawing consent will never reduce the core functionality of the Service to which the processing was not necessary.

For users below the age at which they can give valid consent under applicable law, consent must be given or authorised by a parent or guardian (Section 16).

7.3 Legitimate interests

We process certain data for our legitimate interests, which are: keeping the Service secure and available; preventing fraud and abuse; managing the cost of AI processing through usage limits; understanding in an aggregated way whether the product works; and defending legal claims. Before relying on legitimate interests we balance them against your interests and fundamental rights, taking particular care where users may be children. You may object to processing based on legitimate interests (Section 20).

7.4 Legal obligation

We must keep certain accounting and tax records, respond to lawful orders from courts and authorities, and notify regulators and affected persons of certain data breaches.

7.5 Vital interests and public interest

In rare cases, where necessary to protect someone's life or physical safety and where it is not possible to obtain consent, we may process or disclose limited data. We do not rely on this basis for ordinary operations.

7.6 Special categories and children's data

We do not intentionally process special categories of personal data. Where a user chooses to include such data in study content, it remains on their device and passes through the relay without being stored; the user's act of submitting it is relied on only to deliver the specific answer requested. Children's data receives specific protection throughout this policy.

8. AI Processing and AI Providers

8.1 How AI is used in EdBot

EdBot uses artificial intelligence models to analyse your request and generate structured answers adapted to your level. AI-powered features include the AI Tutor, Explain Mode, the Homework Scanner, PDF conversations, Emergency Mode (turning a deadline and your starting point into a roadmap and practice test), and, as they are released, flashcard, quiz and exam generation, study plans, search and presentations. You are always told when you are interacting with an AI system, and AI-generated content is labelled as such.

8.2 Model routing

EdBot routes each request to the model best suited to its complexity. A simple clarification may go to a smaller, faster model; a multi-step mathematics or programming problem may go to a more capable one. Routing is performed automatically by our server using properties of the request such as its length, type and the feature used. We use the strongest models available to us for each task.

8.3 Our model providers

The categories of model providers we use, and the data each receives, are listed in Appendix B; the names of the current providers are available on request. We select providers that offer commercial API terms under which customer inputs are not used to train their models, and we configure our accounts to the strictest available data-handling settings, including zero data retention where the provider offers it for our use.

8.4 What the provider receives and keeps

- The provider receives the content of each request relayed to it (text, extracted document text, images or audio where applicable) and returns the output.
- The provider is a **processor** acting on our instructions. It may not use your content for its own purposes, including training, except as strictly necessary to provide the service, to keep it secure and to meet legal obligations.

- Providers commonly keep API inputs and outputs for a limited period, often up to about thirty days, solely to detect and investigate abuse and to comply with law, after which they are deleted. Some providers allow this to be reduced or disabled for eligible customers. The retention period that applies to each provider is stated in Appendix B.
- Because that retention is on the provider's systems, we may not be able to delete an individual request on demand during that window, but we can and do ensure that no copy is kept by EdBot.

8.5 Training and improvement of models

EdBot does not train, fine-tune or evaluate AI models on your content, because we do not retain it. We do not authorise our providers to do so. We may test the quality of our service using synthetic or volunteered test material, or with the explicit consent of participants in a pilot.

8.6 Accuracy and limits of AI

AI systems can produce answers that sound confident but are wrong, incomplete or out of date. EdBot cannot guarantee that every answer is correct. To reduce risk, EdBot shows step-by-step explanations, signals uncertainty, prompts you to verify answers where accuracy matters (such as mathematics, science, law, medicine and programming) and, for homework, defaults to hints and an invitation to attempt the problem yourself before showing a full solution. AI output is not professional advice. Please check important results against your teacher, textbook or other reliable sources.

Accuracy is also a data-protection principle: if an AI output contains an incorrect statement about a real person, you may ask us to correct or stop displaying it (Section 20). Because we do not keep outputs, such requests are usually resolved by blocking the offending output for future requests.

8.7 Transparency under AI regulation

In line with the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) and similar rules, we inform users when they are interacting with an AI system, we mark synthetic content where required, and we do not use prohibited practices such as manipulative techniques, exploitation of the vulnerabilities of age, emotion recognition in educational settings, or untargeted scraping of facial images. EdBot is a self-study tool. It is **not** used to decide admission to an educational institution, to formally grade or assess students on behalf of a school, to determine the level of education a person will receive, or to monitor students for prohibited behaviour during tests. If we offer institutional reporting in the future, we will assess whether any use falls into a high-risk category under the AI Act, whose rules for stand-alone high-risk systems currently apply from 2 December 2027, and will update this policy and our controls accordingly.

8.8 Prompt safety

AI systems can be manipulated by text that tries to override their instructions ("prompt injection"). Documents you upload may contain such text. We apply technical measures to reduce the risk, and the relay does not give the AI model access to other users' data or to our systems, because it holds none of your data.

9. Uploads, Documents, Images and the Homework Scanner

9.1 What happens to an upload

When you upload a document or take a photo, the file is first stored in the local database on your device. When you ask EdBot to work with it, the relevant portions (or the extracted text and images) are sent through the relay to the AI provider to generate an answer. The relay does not keep a copy. If you ask a question about the same file again, it is sent again from your device.

9.2 Identifiable material in uploads

Assignments, worksheets, exam papers and photos may contain names, student numbers, photos of people, handwriting, school logos, grades and teachers' comments. Before you upload, consider whether you need to include such details. Where possible, crop or cover names and photos. EdBot does not attempt to identify people in images and does not use facial recognition.

9.3 Other people's information

You must have the right to upload the material you submit. Please do not upload other people's private information, confidential documents of your school or employer, exam materials you are not permitted to share, or content that infringes someone's rights. Do not upload material containing medical records, identity documents, passwords or financial details.

9.4 Exam integrity

EdBot is meant to help you understand and practise. You are responsible for following your school's rules on the use of AI in assessed work. We do not monitor or report your use of EdBot to your school.

9.5 Copyright and ownership

You keep your rights in the material you create or upload. We do not claim ownership of it and, because we do not store it, we do not acquire a licence to keep it. The Terms of Service describe the limited permission you give us to process it for the purpose of providing your request.

10. Storage on Your Device

10.1 How local storage works

EdBot keeps your study data in a local database file in your device's browser or application storage. This storage is specific to a device and browser profile and is not synchronised by EdBot between devices unless we introduce an explicit synchronisation feature, which would be described in an update to this policy and would be optional.

10.2 Your responsibilities

- **Protect your device:** use a screen lock, keep your operating system and browser up to date and do not leave your account signed in on shared or public computers.
- **Back up what matters:** use the export function in the app to save copies of notes and materials you cannot afford to lose. We cannot restore data that is deleted from your device.
- **Shared devices:** if other people use the same device and browser profile, they may be able to see your EdBot data. Use separate browser profiles or sign out.
- **Clearing data:** clearing site data, resetting the browser, uninstalling the web app, using private browsing or certain device clean-up tools may permanently delete your data.
- **Disposal:** when you sell, recycle or give away a device, first delete your EdBot data and sign out.

10.3 Encryption

Data in transit between your device and our relay is encrypted using TLS. The local database relies on the encryption and access protections of your device and browser. We recommend enabling full-device encryption, which is standard on modern phones and available on most computers.

10.4 Access by us

Because the data is on your device, EdBot cannot view, search or recover it. We will never ask you to send us the database file unless you decide to share it with support to fix a problem, in which case it will be used only for that purpose and deleted afterwards.

10.5 Extended history in Premium

Premium offers extended history. Unless and until we announce otherwise, that means a longer or larger history kept in your local database, not a history stored by EdBot.

11. Sharing and Disclosure

We do not sell personal data. We share personal data only in the following situations.

11.1 Service providers (processors)

We use carefully selected providers who process personal data on our behalf, under written contracts that limit their use of the data, require appropriate security and prohibit onward use for their own purposes. Categories include:

Category	Purpose	Data involved
AI model providers	Generate answers, explanations, quizzes and other outputs	Request content in transit; no account identifiers beyond what is necessary
Hosting and delivery platform	Run the website, application and relay; deliver content; collect operational logs	Technical data, account data
Payment processor	Take payments, manage subscriptions, calculate taxes	Payment, billing and subscription data
Email and communications tools	Send service messages and, with consent, newsletters	Email address, name, preferences
Analytics provider	Product analytics without content	Pseudonymous events, device data

Category	Purpose	Data involved
Security, monitoring and error-reporting tools	Detect attacks, outages and errors	Technical data; no request content
Customer-support tools	Manage enquiries	Communications data
Professional advisers	Legal, accounting, audit, insurance	As necessary

The current list of providers is in Appendix B. We will update it before adding a provider that processes personal data in a materially new way, and institutional customers can receive notice of changes in accordance with their agreement.

11.2 Parents, guardians and institutions

If a parent or institution manages your account or plan, they may see account-level information such as your name, plan, status and usage counters. They cannot see your study material, because we do not hold it. Features that would show a parent or teacher progress information are not available today; if introduced, they will be explained clearly before use and will be limited by age and by the choices of the student where the law gives the student that right.

11.3 Other users

EdBot does not publish your profile or study content. Features that let you share material with friends, such as exams with friends, are planned (Section 26). When released, sharing will only occur when you choose to share and will be described precisely in an updated policy.

11.4 Legal requests and protection of rights

We may disclose personal data we hold if we believe in good faith that disclosure is required by law, regulation, court order or lawful request of a public authority; to enforce our terms; to protect the rights, property or safety of EdBot, our users or the public; or to detect, prevent or address fraud, security or technical issues. We examine requests for legality and scope, resist overbroad requests, and, where lawful, notify the affected person. Because we do not hold study content, there is generally nothing in that category to disclose. We publish a transparency report if we receive requests in material numbers.

11.5 Corporate transactions

If EdBot is involved in a merger, acquisition, financing, reorganisation or sale of assets, personal data may be transferred as part of the transaction. We will require the recipient to honour this policy or to give you notice and a choice if its practices would materially differ.

11.6 With your consent or at your direction

We share personal data with others when you ask us to, for example when you export your notes and send them to a teacher.

11.7 Aggregated information

We may share aggregated or anonymised information that does not identify you (Section 6.3).

12. International Data Transfers

12.1 Where data goes

EdBot is operated from Albania and used worldwide. Our providers operate in various countries, including countries in the European Economic Area, the United Kingdom, the United States and elsewhere. Your personal data may therefore be transferred to, stored in and processed in countries other than the one in which you live, including countries whose data protection laws differ from yours and may be less protective.

12.2 Our safeguards

We transfer personal data internationally only where permitted by applicable law and using one of the following mechanisms, as appropriate:

- a decision that the destination ensures an adequate level of protection (for example an adequacy decision of the European Commission or a determination by the Albanian Commissioner);
- **Standard Contractual Clauses** approved by the European Commission, the UK International Data Transfer Agreement or Addendum, and the equivalent Albanian and other national instruments;
- participation of the recipient in a recognised framework, such as the **EU–US Data Privacy Framework** with its UK and Swiss extensions, where the recipient is certified;
- binding corporate rules, codes of conduct or certification mechanisms, where recognised by law; and
- in limited cases, your explicit consent after being informed of the risks, or necessity for performing a contract with you.

We complement these with technical and organisational measures: encryption in transit, strict access controls, minimisation of what is sent (only what is needed to answer your request) and, above all, the fact that EdBot does not keep your content, which greatly reduces what is exposed in any country.

12.3 Transfers from Albania

Law no. 124/2024 permits transfers of personal data from Albania to countries and international organisations that ensure an adequate level of protection, and to other countries where appropriate safeguards such as standard contractual clauses or binding corporate rules are in place, without the need for the Commissioner’s prior authorisation in those cases. We follow those rules.

12.4 Transfers affecting people in the EEA, the UK and Switzerland

Albania does not currently benefit from a general European Commission adequacy decision. Where people in the EEA, the UK or Switzerland provide personal data directly to us, GDPR obligations apply to us directly as a controller under Article 3(2). When we pass that data to processors or sub-processors in third countries, we use the safeguards in Section 12.2. You may request a copy of the relevant safeguards by writing to us.

12.5 Government access

We assess the laws and practices of destination countries, including those on public authority access, when we choose providers and, where necessary, add supplementary measures. We hold very little data that could be demanded, which is the most effective safeguard.

13. Cookies, Local Storage and Similar Technologies

13.1 What these technologies are

Cookies are small text files placed on your device by a website. Related technologies include local storage, session storage, IndexedDB and similar browser storage, pixels and software development kits. We use these technologies for two kinds of purposes: operating the Service, and, with your choice where required, measuring how it is used.

13.2 Categories we use

Category	Purpose	Examples	Consent needed?
Strictly necessary	Sign you in and keep the session secure; remember cookie choices; protect against attacks; load-balance; store your study database on your device and your app preferences	Session or authentication token; CSRF token; consent record; local database; language and theme	No. These are necessary to provide the service you asked for.
Functional	Remember optional preferences that improve your experience	Last-used mode, interface density	Not where strictly necessary; otherwise yes
Analytics	Count visits, measure whether users complete the study loop, find errors in design	Pseudonymous identifier; event counters	Yes, where the law requires it (e.g. EEA, UK)
Advertising / tracking	Not used	None	Not applicable. We do not use advertising cookies.

13.3 Your choices

When you first visit EdBot, a banner lets you accept or reject non-essential technologies with equal prominence, and you can change your choice at any time in Settings. You can also block or delete cookies in your browser, though blocking strictly necessary storage will stop the Service from working, and deleting local storage will delete your study database (Section 10). We honour browser-level signals such as Global Privacy Control as an opt-out of analytics and of any “sale” or “sharing” in the sense of US state laws.

13.4 Cookie list

A detailed list of the cookies and storage items we use, their lifetimes and their providers is in Appendix E.

14. Analytics and Product Measurement

14.1 Why we measure

EdBot's goal is to help students understand and return to practice. To know whether it works, we measure things like: the share of new users who go from question to saved material to practice in one session (loop completion); activation; return visits; and the share of users who practise after an explanation. We need these measurements to improve the product, to decide which features to keep and to report results in aggregate to partners and funders.

14.2 What is measured

- Event names and timestamps (for example "practice_started");
- The feature or mode used and the type of file (but not its content or file name);
- A pseudonymous identifier that is not your name or email address;
- Coarse device and location information (country level, browser, screen size); and
- Performance data such as load time and errors.

14.3 What is not measured

Analytics events never include the text of your questions, answers, notes or uploads, the names of your documents, your quiz answers or your scores in a form that would reveal what you studied. We do not use session-replay tools that record your screen or keystrokes. We do not enable features that fingerprint your device.

14.4 Tools and settings

We use a privacy-focused analytics provider configured with IP truncation or anonymisation, no use of the data by the provider for its own purposes and a retention limit of 14 months. Where the law requires consent, the tool is not loaded until you opt in.

14.5 Aggregate reporting

Results shared outside EdBot, such as with accelerators, funders, schools or research partners, are aggregated, and small groups are suppressed so that individuals cannot be singled out.

15. Payments and Subscriptions

15.1 Plans

EdBot offers a Free plan with daily limits, a Premium plan billed monthly or annually, and institutional plans. Prices are shown in euros before you buy and may be adjusted by region. Subscriptions renew automatically until cancelled; the Terms of Service and the checkout page explain renewal, cancellation and refund rights, including statutory rights of withdrawal for consumers.

15.2 Payment processing

Payments are handled by a third-party payment provider (see Appendix B), which acts as an independent controller for its own regulatory purposes (such as anti-money-laundering and fraud prevention) and as our processor for other purposes. Card details are entered directly on the provider's page or in its embedded fields and are not seen by EdBot. The provider's privacy notice applies to its own processing.

15.3 What we keep

We keep a record of each transaction (date, amount, plan, status, customer reference and invoice) for as long as accounting and tax law requires, even if you delete your account. This record does not include what you studied.

15.4 Parents and payers

Where a parent or guardian pays for a student's Premium plan, the payer's billing information is processed for payment only and is not combined with the student's study content, which EdBot does not hold.

15.5 Taxes and fraud checks

We and our payment provider process country, postal code and tax identification information to calculate sales tax or VAT and to comply with tax law. We may use fraud-detection tools to protect against stolen cards and chargebacks; these may involve limited automated decisions about whether to accept a payment, in which case you can ask for a person to review the decision.

16. Children and Teens

16.1 Who EdBot is for

EdBot is intended for secondary-school students, university students and adult learners. Because many of our users are minors, we apply heightened care. We design the Service so that the information about children that we hold is minimal and so that children's interests are placed first.

16.2 Minimum age

You must be at least 13 years old to create an EdBot account. We do not knowingly collect personal data from children under that age. If we learn that we have done so, we will delete the account and the associated data promptly. If you believe a child under that age has registered, please contact us.

16.3 Parental permission

In many countries a child must be above a certain age (the "digital age of consent") before they can validly consent to data processing by an online service, and below that age a parent or guardian must give or authorise it. That age is **13** in the United States, between **13 and 16** in EU Member States, **13** in the United Kingdom, and, for users in Albania, 16 as a precaution unless and until Albanian law is confirmed to set a lower age for consent to online services. We therefore ask users who are below the applicable age to have a parent or guardian's permission,

and we use reasonable means, proportionate to the risk and to the minimal data we hold, to check that permission has been given. Teenagers above that age but under 18 are encouraged to involve a parent or guardian.

16.4 Design for young people

- **Data minimisation by default:** we hold only minimal account data and no content.
- **No advertising, no profiling for marketing,** no sale of data and no nudging techniques that encourage excessive use or the disclosure of more data.
- **Default privacy:** the most protective settings are on by default; analytics for under-age users are limited to what is strictly necessary and, where consent is required, are off until a parent or guardian agrees.
- **Plain language:** privacy information and prompts are written to be understood by teenagers; a short young-person version of this policy is available on request.
- **Learning-first answers:** homework defaults to hints and an attempt by the student before a full solution, supporting learning rather than copying.
- **Safety signals:** the Service is designed to respond with care and to point to appropriate help if a young person expresses distress (Section 23).
- **No contact with strangers:** EdBot has no open chat or public profiles. Planned sharing features are limited to people you invite.

16.5 Rights of parents and guardians

A parent or guardian of a minor may contact us to ask what account data we hold about their child, to correct or delete it, to withdraw consent they gave and to close the account. We may need to verify the relationship and the child's identity. As we hold no study content, the child's notes and conversations can be reviewed and deleted on the child's own device. Where the child has reached an age at which the law gives them rights of their own, we will take their wishes and best interests into account.

16.6 United States: COPPA

EdBot does not direct the Service to children under 13 and does not knowingly collect personal information from them. If we ever allow users under 13 in the United States, we will first obtain verifiable parental consent in accordance with the Children's Online Privacy Protection Act and the FTC's amended COPPA Rule, which has required operators to comply with its new provisions since 22 April 2026, and we will publish a children's privacy notice.

16.7 Reporting concerns

If you are a parent, teacher or young person with a concern about how EdBot treats children's data, please write to edbotsupp@gmail.com with "Child safety" in the subject line. We treat these reports as a priority.

17. Schools, Course Centres and Institutional Plans

17.1 Status of institutional plans

Institutional plans (for schools, course centres and organisations) are planned for a later phase and will start only after we have evidence from individual use and clear privacy requirements. This section sets out how we intend to operate so that institutions and students know what to expect.

17.2 Roles

In an institutional deployment, the institution will normally be the **controller** of its students' personal data, and EdBot will be a **processor** acting on its instructions under a data processing agreement. For its own purposes (security, billing, product improvement using non-content data, legal compliance) EdBot remains an independent controller of limited account and technical data.

17.3 What an institution can and cannot see

- An institution can manage seats, plan status and active-user counts.
- **Limited reporting**, if offered, will use only data that students or the institution have chosen to share and that is lawful to share, and will be described to students beforehand.
- An institution cannot use EdBot to read students' private conversations, notes or uploads, because EdBot does not hold them.

17.4 Institutional obligations

The institution is responsible for having a lawful basis to use EdBot with its students, for providing its students and their parents with any notices required, for obtaining any required consents, for complying with rules on student records and on assessment, and for configuring accounts appropriately.

17.5 FERPA and similar student-record laws

Where EdBot receives education-record information from a US school or district, we will do so as a "school official" with a legitimate educational interest under the Family Educational Rights and Privacy Act (FERPA), under the school's direct control, and we will use the information only for the educational purposes the school authorises. We will comply with applicable state student-privacy laws and sign recognised student-data-privacy agreements on request. Equivalent commitments will be offered under the education and children's laws of other countries.

17.6 Deletion at the end of the contract

At the end of an institutional contract we will return or delete institutional account data within 60 days, subject to legal retention duties.

18. Data Retention

18.1 Principle

We keep personal data only as long as necessary for the purposes for which it was collected, including to satisfy legal, accounting or reporting requirements. When we no longer need it, we delete it or irreversibly anonymise it. For the data stored on your device, you decide.

18.2 Retention schedule

Data	Retention period	Notes
Study content (conversations, uploads, notes, flashcards, quizzes, progress)	Not held by EdBot. On your device until you delete it.	Section 10
Request content relayed to AI models	Not retained by EdBot. Provider retention: see Appendix B (up to 30 days, or none where zero retention is available).	Section 8
Account and profile data	While your account is active, then deleted within 30 days of closure	Backups overwritten within 35 days
Inactive accounts	Closed after 24 months of inactivity after notice by email	To minimise data held
Subscription, invoice and payment records	As required by Albanian accounting and tax law and by the law of other countries where we are registered (generally several years)	Legal obligation; does not contain study content
Usage counters	Rolling period of 35 days	Needed for limits
Technical and security logs	30 to 90 days; longer only for an investigation of an incident	No request content
Analytics events	14 months, then aggregated or deleted	Pseudonymous
Consent and preference records	While active plus the limitation period for claims	Proof of compliance
Support and complaints correspondence	24 months after case closure	Longer if litigation
Newsletter data	Until you unsubscribe, plus a suppression record to honour the opt-out	
Pilot and interview data	As stated in the participant information sheet; recordings deleted within 6 months of transcription	Section 25
Data subject request records	3 years	Accountability
Breach register	5 years	Legal obligation

18.3 Legal holds

If we are subject to a legal duty or a legitimate need to preserve information, such as a lawful order, litigation or an investigation of fraud, we may retain relevant data beyond these periods for as long as necessary.

18.4 Deletion in practice

When we delete data, we remove it from live systems and schedule its removal from backups, which are overwritten on a rolling cycle. Until backups are overwritten the data is isolated and not used. Deletion of account data does not delete your local database; you should delete that separately in the app or by clearing your browser data (Section 10).

19. Data Security

19.1 Our approach

We implement technical and organisational measures that are appropriate to the risk, taking account of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as required by Law no. 124/2024, Article 32 GDPR and equivalent laws. Our approach starts with data minimisation: information we do not hold cannot be lost.

19.2 Measures

Area	Measures
Minimisation and design	Local-first architecture; no content archive; privacy by design and by default; data protection impact assessment for new features
Encryption	TLS for all traffic; encryption at rest for account data and backups; secure hashing with salt for passwords
Secrets	AI provider credentials kept server-side in a secrets manager and never exposed to the client; keys rotated; least privilege
Access control	Role-based access; multi-factor authentication for administrative accounts; logging of administrative access; prompt removal of access when roles change
Application security	Secure development practices; dependency scanning; code review; input validation; protection against injection, cross-site scripting and request forgery; rate limiting
Infrastructure	Reputable cloud and edge providers with recognised certifications; network segregation; vulnerability patching; monitoring and alerting
Logs and error reporting	Request content is excluded; log access restricted; short retention
People	Confidentiality obligations; training on privacy and security; need-to-know access
Providers	Due diligence; contracts with security and confidentiality terms; monitoring of sub-processors
Resilience	Backups of account data; incident response and recovery plans; periodic testing
Review	Periodic security review and, as the company grows, independent penetration testing

19.3 Your role

Choose a strong, unique password, do not share it, enable multi-factor authentication where available, keep your device secure and tell us immediately if you suspect unauthorised access to your account.

19.4 Personal data breaches

If a personal data breach occurs that is likely to result in a risk to your rights and freedoms, we will notify the competent supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it, as Law no. 124/2024 and the GDPR require. If the breach is likely to result in a high risk to you, we will also inform you directly, without undue delay, in clear and plain language, describing what happened, what data is concerned, the likely consequences and what we are doing and what you can do about it. We keep a record of all breaches.

19.5 Residual risk

No online service is completely secure. Our local-first design reduces the consequences of a breach on our side, but it cannot protect data on a compromised device. Please tell us promptly of any vulnerability you find; we welcome responsible disclosure at edbotsupp@gmail.com.

20. Your Rights and How to Exercise Them

20.1 Your rights

Depending on where you live, you have some or all of the following rights. We extend the core rights below to every user worldwide, as a matter of good practice.

Right	What it means	How it works at EdBot
Information	To be told how your data is used	This policy and in-product notices
Access	To confirm whether we process your data and obtain a copy and information about processing	We provide a copy of the account data we hold. Study content is on your device, so you can see it in the app and export it.
Rectification	To correct inaccurate or incomplete data	Edit most details in Settings, or ask us
Erasure (“right to be forgotten”)	To have data deleted where legal grounds apply	We delete your account data on request subject to legal retention (e.g. invoices). You delete local data in the app.
Restriction	To ask us to pause processing while a dispute is resolved	Available where the legal conditions are met
Portability	To receive data you provided in a structured, commonly used, machine-readable format and transmit it to another service	Account data export; export of notes and materials from your device in open formats
Objection	To object to processing based on legitimate interests or to direct marketing	Opt-out of analytics and marketing in Settings; other objections by request
Withdraw consent	To withdraw consent at any time	Settings or request
Not to be subject to solely automated decisions	To human review of decisions with legal or similarly significant effects	We make none (Section 22), except possibly payment-fraud checks
Complain	To lodge a complaint with a supervisory authority	Section 29

20.2 How to make a request

1. Email edbotsupp@gmail.com from the address linked to your account, or use the form in Settings under “Privacy”.
2. Say which right you want to exercise and give enough detail for us to find your data. A template is provided in Appendix C.
3. We may ask for information to verify your identity. We will ask only for what is necessary and will not require more personal data than the account already holds.
4. If you act through an authorised agent or as a parent or guardian, we may ask for proof of authority.

20.3 Our response

We respond **without undue delay and within one month** of receiving a valid request. We may extend that period by up to two further months where necessary, taking into account the complexity and number of requests; we will tell you within the first month and explain why. Some laws set a different period (for example 45 days under certain US state laws); we apply the period that gives you the stronger protection.

20.4 Cost

Requests are free of charge. If a request is manifestly unfounded or excessive, in particular if repetitive, we may charge a reasonable fee or refuse to act, and will explain why.

20.5 Limits

Rights are not absolute. We may refuse or limit a request where the law allows or requires, for example where it would adversely affect the rights of others, where we are required to keep the data, or where we cannot identify you. We cannot access, correct or delete data that only exists on your device, but you can do so yourself. If we refuse, we will explain the reason and tell you how to complain.

20.6 Your choices without making a request

- **Delete study data:** Settings > Data > Delete local data.
- **Export:** Settings > Data > Export.
- **Cookies and analytics:** Settings > Privacy.
- **Marketing:** unsubscribe link in any email or Settings > Notifications.
- **Delete account:** Settings > Account > Delete account.

20.7 Non-discrimination

We will not discriminate against you for exercising your rights, for example by denying the Service, charging different prices or providing a lower quality, except where the difference is directly related to the data that is needed to provide the feature.

21. Regional Supplements

EdBot is offered globally. This section describes additional information and rights for people in particular places. If you are in more than one of these categories, all that apply to you apply. Where a supplement gives you a stronger right than the rest of this policy, the stronger right applies to you.

21.1 Albania

EdBot is established in Albania, and processing of personal data by us is governed by **Law no. 124/2024 "On the Protection of Personal Data"**, which entered into force in February 2025, repealed Law no. 9887/2008 and aligns Albanian law with the GDPR. We also take into account Article 35 of the Constitution of the Republic of Albania (protection of personal data), the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data to which Albania is a party, the Law on Electronic Commerce (no. 10128/2009), the Law on Electronic Communications (no. 9918/2008) in relation to electronic marketing and the confidentiality of communications, the Law on Cyber Security (no. 2/2017), the consumer protection legislation and the Law on the Rights and Protection of the Child (no. 18/2017), together with the binding instructions issued by the Commissioner, including on education and direct marketing.

- **Supervisory authority:** the Commissioner for the Right to Information and Protection of Personal Data (Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale), Tirana, website idp.al.
- **Your rights** under Law no. 124/2024 include information, access, rectification, erasure, restriction, portability, objection and not to be subject to solely automated decisions, and the right to complain to the Commissioner and to seek judicial remedies.
- **Notifications:** where Albanian law requires us to register, notify or consult the Commissioner (for example on the appointment of a data protection officer, transfers or breaches), we do so.
- **Language:** Albanian users may request this policy and our responses in Albanian.
- **Pilot:** the local student and teacher pilot in Albania will be run under a separate information sheet and with parental consent for minors.

21.2 European Economic Area

If you are in the EEA, the GDPR applies to our processing of your data because we offer the Service to you. We are the controller (Section 2). Our legal bases are in Sections 6 and 7. You have the rights in Section 20 and the right to lodge a complaint with the supervisory authority of the Member State where you live, work or where an alleged infringement occurred; a list of authorities is on the website of the European Data Protection Board. Our EU representative is named in Section 2.3. Because we offer an electronic communications-related service using cookies and similar technologies, we also follow the ePrivacy Directive as implemented in your country. Our transfers are described in Section 12.

Digital consent age. Member States set the age of digital consent between 13 and 16 (Article 8 GDPR). For users below that age in your country, we require parental authorisation (Section 16).

21.3 United Kingdom

If you are in the UK, the UK GDPR, the Data Protection Act 2018 and the Privacy and Electronic Communications Regulations apply. You can complain to the Information Commissioner's Office (ico.org.uk). Our UK representative is named in Section 2.3. We design EdBot with regard to the ICO's Age Appropriate Design Code (the Children's Code) and its fifteen standards, including data minimisation, high-privacy defaults, no detrimental use of children's data and age-appropriate transparency. UK users aged 13 or over can give their own consent for online services. Data protection reforms under UK legislation are being implemented over time, and we will follow them.

21.4 Switzerland and Liechtenstein

If you are in Switzerland, the revised Federal Act on Data Protection (FADP) applies. You can complain to the Federal Data Protection and Information Commissioner (edoeb.admin.ch). We use the Swiss-approved transfer safeguards and the Swiss–US element of the Data Privacy Framework where applicable.

21.5 United States (general)

EdBot is not directed at children under 13 (Section 16). We do not sell personal information and do not share it for cross-context behavioural advertising. We do not knowingly process "sensitive personal information" as defined by US state laws, other than incidentally in content that stays on your device. Residents of US states with comprehensive privacy laws (including California, Colorado, Connecticut, Virginia, Utah, Texas, Oregon and others) have the rights to know/access, correct, delete, obtain a portable copy, and opt out of targeted advertising, sales and certain profiling, and to appeal a refusal. We honour these rights for all US users, subject to the legal thresholds of each law. To appeal a decision, reply to our response with "Appeal" in the subject line; we will respond within the period required by your state's law, and if you are not satisfied you may contact your state attorney general.

21.6 California

This section supplements the above for California residents under the California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA). The CCPA applies only to businesses that meet certain thresholds; we honour these rights for California residents whether or not those thresholds apply to us.

CCPA category collected in the last 12 months	Collected?	Source	Disclosed for a business purpose to
Identifiers (email, display name, account ID, IP address)	Yes	You; your device	Hosting, email, analytics and payment providers
Customer records (billing information)	Yes, via payment processor	You; payment processor	Payment processor
Commercial information (plan, purchase history)	Yes	You; payment processor	Payment processor
Internet or network activity (usage events, logs)	Yes	Your device	Hosting, analytics and monitoring providers
Geolocation	Country-level only, inferred from IP	Your device	Hosting and analytics providers
Audio, visual or similar information	Only when you use a feature that sends it, in transit	You	AI model providers, not retained by EdBot

CCPA category collected in the last 12 months	Collected?	Source	Disclosed for a business purpose to
Education information	Not retained by EdBot; in transit only	You	AI model providers
Inferences	No profiles built about individuals	N/A	N/A
Sensitive personal information	No (incidental only, on-device and in transit)	N/A	N/A

- We have not sold or shared personal information in the preceding 12 months, and do not knowingly sell or share the personal information of consumers under 16.
- We retain each category for the periods in Section 18.
- You may exercise rights through the methods in Section 20; you may designate an authorised agent; we will verify your identity and the agent's authority.
- We recognise opt-out preference signals such as Global Privacy Control.
- California's "Shine the Light" law lets residents ask which personal information is disclosed to third parties for their direct marketing; we make no such disclosures.
- Under the California Online Privacy Protection Act, we tell you that Section 13.3 describes how we respond to browser signals such as Global Privacy Control.

21.7 Student-privacy laws in the United States

If EdBot is used through a school, FERPA and state student-data laws (such as California's SOPIPA and Education Code provisions) may apply to the school and to us as its service provider. We do not use student information for targeted advertising, do not build profiles for non-educational purposes, do not sell student information, and delete it at the school's direction (Section 17).

21.8 Canada

If you are in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) and provincial laws (including Quebec's Law 25, Alberta and British Columbia PIPA) may apply. You may access and correct your personal information and complain to the Office of the Privacy Commissioner of Canada or the provincial authority. For Quebec, we conduct privacy impact assessments for transfers outside Quebec; the person responsible for the protection of personal information can be reached at the address in Section 2.

21.9 Australia and New Zealand

If you are in Australia, we handle personal information in line with the Australian Privacy Principles in the Privacy Act 1988 and will follow the Children's Online Privacy Code when it applies. You may complain to the Office of the Australian Information Commissioner. If you are in New Zealand, the Privacy Act 2020 applies and you may complain to the Office of the Privacy Commissioner.

21.10 Brazil

If you are in Brazil, the General Personal Data Protection Law (LGPD) applies. Our legal bases are those in Section 7 as recognised by the LGPD. Processing of children's and adolescents' data is done in their best interest and, for children, with specific consent from at least one parent or legal guardian. You may contact the National Data Protection Authority (ANPD) and our contact point in Section 2.

21.11 India

If you are in India, the Digital Personal Data Protection Act, 2023 applies. We process the data of a person under 18 only with verifiable consent of a parent or lawful guardian, and we do not track, behaviourally monitor or target advertising at children. You have the rights of access, correction, erasure, grievance redressal and nomination. You can contact our grievance contact in Section 2 and, if unresolved, the Data Protection Board of India.

21.12 Western Balkans, Turkey and Southeast Europe

EdBot expects many early users in Albania and neighbouring countries. Kosovo, North Macedonia, Montenegro, Serbia, Bosnia and Herzegovina and Türkiye have data protection laws that are, to varying degrees, aligned with the GDPR (in Turkey, Law no. 6698, KVKK). We apply the protections in this policy to users in these countries and respect the specific rights, authorities and language requirements of their laws. You may complain to your national supervisory authority.

21.13 Asia-Pacific, Middle East and Africa

For users in Japan (Act on the Protection of Personal Information), South Korea (Personal Information Protection Act, which requires a legal guardian's consent for children under 14), Singapore (PDPA), the United Arab Emirates and Saudi Arabia (their respective personal data protection laws), South Africa (POPIA) and other countries not listed, we process data according to this policy and the mandatory local requirements that apply to us. If local law gives you additional rights or requires additional notices, please contact us and we will honour them to the extent they apply. EdBot is not specifically offered in mainland China.

22. Automated Decision-Making and Profiling

EdBot uses automated systems to generate answers and to personalise the difficulty and format of explanations. Personalisation takes place on your device using your own progress data and does not produce legal effects or similarly significant effects on you.

- **No automated decisions with legal effect.** We do not make decisions based solely on automated processing that produce legal effects concerning you or similarly significantly affect you, for example denying access to education, grading you for a school or deciding on employment.
- **Progress dashboard.** Scores, streaks and recommendations are informational study aids for you. They are not official assessments, are not shared with schools or parents unless a feature that you or your guardian have chosen says so, and should not be treated as evidence of ability.

- **Usage limits and abuse detection.** We apply automated rules to enforce limits and block abusive traffic. If an automated rule wrongly blocks you, contact us and a person will review it.
- **Fraud checks on payments** may involve automated scoring by our payment provider (Section 15.5). You can request human review.
- **No profiling for marketing or advertising.**

23. Safety, Abuse Prevention and Content Moderation

23.1 Why we check requests

We need to prevent the Service being used to generate harmful content, to attack our systems or to evade usage limits. We use a combination of rate limiting, behavioural signals about traffic patterns (not content), automated checks in memory on requests as they pass through the relay and safety systems of our AI providers.

23.2 What is kept

Automated safety checks operate in memory. If a request is blocked, we keep a minimal event record (time, account or device identifier, category of rule triggered) for 30 days to investigate abuse. We do not keep the text of the request. Our AI providers may keep flagged requests under their own policies (Appendix B).

23.3 Wellbeing of young people

Young people sometimes tell a chatbot about stress, loneliness or worse. EdBot is a study tool and not a counselling or emergency service. Where a message suggests that someone may be at risk of harming themselves or being harmed, EdBot is designed to respond with care and to encourage the person to talk to a trusted adult or a local helpline. This is done automatically at the moment of the request; because we do not retain content, we cannot see or follow up on these messages, and no one at EdBot reads them. If you are in danger, please contact your local emergency number straight away.

23.4 Illegal content and law-enforcement duties

We do not tolerate the use of EdBot to create or request child sexual abuse material or other content that is illegal. We will take the steps the law requires, including cooperating with authorities and reporting to the competent bodies, and we may preserve the minimum information necessary for that purpose.

23.5 Reporting

If you see an answer that is harmful, wrong or inappropriate, use the in-app “Report” button, which sends us only what you choose to include, or write to us.

24. Marketing Communications

We send **service messages** (account, security, payment, legal updates) because they are part of the Service. We send **marketing messages** only if you have agreed to receive them or where the law allows us to contact existing customers about similar services with an easy way to opt out. Every marketing message has an unsubscribe link. We do not send marketing to children under the age at which they can lawfully consent unless a parent has agreed. We do not buy or rent marketing lists. Our promotional activities on social media, creator and campus partnerships and referral programmes use public information and information you give us for that purpose, and partners are not given your email address without your consent.

25. Research, Pilots and Feedback

We run structured pilots and user research, in Albania and elsewhere, with students and teachers, to learn whether EdBot helps. Participation is voluntary. Before you take part, you will receive an information sheet explaining who is running the research, what will be collected, why, how long it will be kept, who sees it and how to withdraw. For minors, we ask for the permission of a parent or guardian and for the minor's own agreement. We collect the minimum, pseudonymise where possible, and report results only in aggregate. You may withdraw at any time without consequence, and we will delete your data unless it has been irreversibly anonymised. Interview recordings are used only to take notes and are deleted as stated in Section 18. Your use of the Service does not depend on joining a pilot.

26. Features Under Development

Our plans include additional features. This policy describes how EdBot works today. Before any of the following goes live to the public, we will update this policy, tell you if the change is material, assess privacy risks and, where required, ask for your consent.

Planned feature	Likely privacy implications	What we will do
Exams with friends / shared exams and referrals	Sharing of exam content or invitations between users; invitee email addresses; possible results sharing	Share only on your action; explain exactly what travels and where it is stored; limited to invited people; no public profiles; easy revoke
Voice	Audio of your voice processed by a speech-recognition and synthesis provider; microphone permission	Audio processed in transit; no voiceprints; permission prompts; clear indication when listening; not retained by EdBot
Search	Search queries and retrieved pages involve search providers; links to external sources	Name the search provider; avoid including identifiers; show sources
Presentations and PDF output	Generation of files from your material; export to your device	Generated on request; delivered to your device; not stored by EdBot
Extended history and sync	If history is ever synchronised or backed up in the cloud, EdBot would store content	Optional, opt-in, end-to-end encryption where feasible, with a clear update to this policy and a separate consent
Family plan	Parent and child accounts; the parent's view of the child's activity	Explain what the parent can see; keep to what is necessary; respect the child's growing rights

Planned feature	Likely privacy implications	What we will do
Institutional packages and limited reporting	Controller-processor relationship; institutional visibility of progress	Data processing agreement; student notice; evaluate AI Act risk category (Section 8.7)

27. Third-Party Links and Services

EdBot may display links to external websites and sources, for example when search or citations are available. We do not control and are not responsible for their privacy practices. We recommend that you read their policies. Content from third-party sites that you open is not covered by this policy. If you sign in with a third-party identity provider, the provider's terms and privacy policy apply to its own processing.

28. Changes to This Policy

We may update this policy to reflect changes in our practices, the Service, technology or the law. When we do, we change the "Last updated" date and version number. If the change is material, we will provide prominent notice, for example by email or an in-app message, at least 30 days before it takes effect where possible, and we will seek your consent again where the law requires it. Please review the policy periodically. Previous versions are kept and will be provided on request.

Version	Date	Summary of changes
1.0	19 October 2026	First full publication.

29. Contact, Complaints and Supervisory Authorities

29.1 Contact us first

We would like the chance to resolve your concern. Write to edbotsupp@gmail.com. Please say which country you are in so that we can apply the right law. We will acknowledge your message and aim to resolve complaints within one month.

29.2 Supervisory authorities

You always have the right to complain to a data protection authority. You are not required to contact us first.

Where	Authority	Website
Albania	Commissioner for the Right to Information and Protection of Personal Data (IDP)	idp.al
EEA	Your national data protection authority (list kept by the European Data Protection Board)	edpb.europa.eu
United Kingdom	Information Commissioner's Office	ico.org.uk
Switzerland	Federal Data Protection and Information Commissioner	edoeb.admin.ch
United States	Federal Trade Commission; your state attorney general	ftc.gov

Where	Authority	Website
Canada	Office of the Privacy Commissioner of Canada	priv.gc.ca
Australia	Office of the Australian Information Commissioner	oaic.gov.au
Brazil	Autoridade Nacional de Proteção de Dados (ANPD)	gov.br/anpd
Other countries	Your national authority	-

29.3 Jurisdiction and governing law

This policy is governed by the laws of the Republic of Albania, without prejudice to mandatory data-protection and consumer-protection rights that you have in the country where you live, and to your right to bring proceedings in the courts of that country.

30. Glossary

Term	Meaning
AI model / provider	A machine-learning system that generates answers, and the company that operates it.
Anonymisation	Making data so that a person cannot be identified by any means reasonably likely to be used.
Commissioner	The Albanian Commissioner for the Right to Information and Protection of Personal Data.
Consent	A freely given, specific, informed and unambiguous indication of agreement by clear affirmative action.
Controller / Processor	The party that determines purposes and means of processing / the party that processes on the controller’s behalf.
COPPA	The US Children’s Online Privacy Protection Act.
DPO	Data Protection Officer.
EEA	The European Economic Area: EU Member States plus Iceland, Liechtenstein and Norway.
FERPA	The US Family Educational Rights and Privacy Act.
GDPR	Regulation (EU) 2016/679, the General Data Protection Regulation.
Local database	A database file stored in your device’s browser or application storage.
Personal data	Information about an identified or identifiable person.
Processing	Any operation on personal data, such as collecting, storing, using or deleting it.
Pseudonymisation	Processing so that data can no longer be attributed to a person without additional information kept separately.
Relay	EdBot’s server component that forwards requests to AI providers without storing them.
SCCs	Standard Contractual Clauses for international transfers.
Service	The EdBot website, application, relay and related services.
Sub-processor	A provider engaged by a processor.

Appendix A: Data Inventory

Data and examples	Source	Purpose and basis	Where kept	Retention
Email, display name, authentication data	You; identity provider	Account (contract); security (legitimate interests)	EdBot account database	Life of account + 30 days
Age band / age confirmation, country, language	You; browser	Age protections (legal obligation, legitimate interests); localisation (contract)	Account database	Life of account + 30 days
Plan, subscription status, customer reference, invoices	You; payment provider	Contract; legal obligation	Payment provider; EdBot records	Statutory period for invoices
Usage counters	Generated by Service	Enforce limits (legitimate interests, contract)	EdBot database	35 days rolling
IP address, device and browser data, request metadata	Your device	Security and delivery (legitimate interests)	Hosting platform logs	30-90 days
Analytics events (no content)	Your device	Product measurement (consent / legitimate interests)	Analytics provider	14 months
Support and complaint messages	You	Support (contract, legitimate interests)	Email and support tools	24 months after closure
Newsletter and referral data	You	Marketing (consent)	Email tool	Until unsubscribe
Pilot data	You	Research (consent)	Research storage	Per information sheet
Conversations, uploads, notes, flashcards, quizzes, progress	You	Your own study (you control)	**Your device only**	Until you delete
Request content in transit	You	Answer your request (contract)	Memory of relay; AI provider	Not retained by EdBot; provider per Appendix B

Appendix B: Service Providers and Sub-processors

We list our providers by category and by the data they handle. The names of the current providers are available on request at edbotsupp@gmail.com. We bind each provider by contract to process personal data only on our instructions and to keep it secure.

Category	Role	Data	Retention and safeguards
AI model providers (commercial large-language-model APIs)	Generate answers for the AI Tutor and other AI features, including alternative models used for routing	Request content in transit	Up to 30 days or less depending on provider and settings; none where zero retention is available; no training on API data; SCCs or Data Privacy Framework for transfers
Hosting and delivery platform (Vercel Inc.)	Hosting, edge network, relay execution, operational logs	Technical data; transient request data	Logs 30 to 90 days; request bodies excluded; SCCs or Data Privacy Framework
Payment processor	Payments, subscriptions, tax calculation, fraud prevention	Billing and subscription data	As required by financial and tax law; own privacy notice

Category	Role	Data	Retention and safeguards
Email provider	Service and marketing email	Email address, name	Until you unsubscribe or close your account
Analytics provider	Product analytics without content	Pseudonymous events	14 months; IP truncation
Error-monitoring and security tools	Error reports, attack detection	Technical data; no request content	Short retention
Speech, search and other providers (when launched)	Voice and search features	Audio; queries	To be added before the feature launches

Appendix C: Template for Making a Privacy Request

You can copy and send the text below to edbotsupp@gmail.com. You do not have to use it.

Template

Subject: Privacy request: [access / correction / deletion / export / objection / withdraw consent / other]

Hello EdBot team,

I am the holder of the account associated with this email address. I would like to exercise the following right: [describe]. Details that may help you: [country; what you want changed or deleted; dates].

If I am making this request on behalf of a child or another person, I am their [parent / guardian / authorised agent] and can provide proof if needed.

Please confirm receipt and reply within the legal time limit.

Thank you, [name]

What to expect

1. We confirm receipt, usually within five working days.
2. We verify your identity using details already linked to your account.
3. We search the account data we hold. Remember that study content is on your device.
4. We reply within one month (extendable as explained in Section 20.3) with the result and, if applicable, reasons for refusal and how to complain.

Appendix D: Summary of the Legal Framework

Instrument	Relevance to EdBot
Albanian Law no. 124/2024 on the Protection of Personal Data	Primary law for the controller in Albania; GDPR-aligned; extraterritorial reach; rights, breach notification, DPO, transfers, sanctions
Constitution of Albania, Art. 35	Constitutional protection of personal data
Council of Europe Convention 108	International privacy treaty to which Albania is a party
Albanian Laws on Electronic Commerce (10128/2009), Electronic Communications (9918/2008), Cyber Security (2/2017), Child Rights (18/2017) and consumer protection	Information duties, electronic marketing, security and children’s protection

Instrument	Relevance to EdBot
Regulation (EU) 2016/679 (GDPR) and ePrivacy Directive	Applies to offers to people in the EEA; cookies and marketing rules
Regulation (EU) 2024/1689 (AI Act), as amended by the 2026 Digital Omnibus	Transparency duties for AI interaction and content; prohibited practices; high-risk education systems under Annex III apply from 2 December 2027; general-purpose AI obligations already apply to model providers
UK GDPR, Data Protection Act 2018, PECR, Children's Code	UK users
Swiss FADP	Swiss users
COPPA (amended Rule, compliance since 22 April 2026), FERPA, state privacy and student-privacy laws, CCPA/CPRA	US users and school deployments
PIPEDA and Quebec Law 25; Australian Privacy Act; NZ Privacy Act 2020; LGPD; India DPDP Act 2023; KVKK; Japan APPI; Korea PIPA; Singapore PDPA; POPIA; Gulf laws	Other regions as described in Section 21

Appendix E: Cookies and Local Storage Items

Name / item	Provider	Category	Purpose	Lifetime
Session token	EdBot	Strictly necessary	Keeps you signed in	Session / 30 days
Anti-forgery token	EdBot	Strictly necessary	Protects against request forgery	Session
Consent record	EdBot	Strictly necessary	Remembers your cookie choices	12 months
Local database (browser storage)	EdBot (on your device)	Strictly necessary	Stores your study data on your device	Until you delete it
Preferences (language, theme, mode)	EdBot	Strictly necessary / functional	Remember interface settings	12 months
Analytics identifier	Analytics provider	Analytics (consent)	Counts visits and loop completion	13 months

End of policy

Thank you for reading. If anything is unclear, please write to us. We would rather answer a question than leave a doubt.