Privacy Policy

EduBase Educational Services Limited Liability Company
Last revision: 23rd October 2026

[1.] Who processes your data?

[1.1.] **Controller**: EduBase Oktatási Szolgáltató Korlátolt Felelősségű Társaság (EduBase Educational Services Limited Liability Company; “EduBase”, “we”).

- Registered seat and postal address: 1046 Budapest, Pálya utca 24. 4. em. 20., Hungary
- Company registration number: 01-09-284426
- Tax number: 25598386-2-41
- E-mail: info@edubase.net

[1.2.] **Data Protection Officer**: dpo@edubase.net, or by post at the address above, marked “Data Protection Officer”. You can also use the data protection category of the Contact form on our main page.

[1.3.] **Scope**. This Policy applies to personal data processed in connection with the use of edubase.net and its subdomains, the eduba.se and ebs.to URL shortening services, the EduBase mobile applications, the API and the MCP server. For services provided on dedicated instances (versions of the Service installed separately for one customer and not shared with other customers), a different notice published there may also apply.

[1.4.] **Applicable legislation**:

- the General Data Protection Regulation (EU) 2016/679 (GDPR);
- Hungarian Act CXII of 2011 on the right to informational self-determination and on the freedom of information (Infotv.);
- Hungarian Act C of 2003 on electronic communications (cookies);
- Hungarian Act XLVIII of 2008 on the basic conditions and certain restrictions of commercial advertising activities (Grt., newsletter);
- Hungarian Act C of 2000 on accounting (Sztv.);
- Regulation (EU) 2024/1689 (AI Act).

[2.] Our two roles: controller and processor

EduBase is used by individuals and by organizations (companies, schools, universities, training providers), so whether we or the organization decide on the processing of your data depends on the purpose for which the data entered the system.

Situation	Who decides on the processing?	Whom should you contact?
You registered yourself, create your own content, practice or take quizzes	EduBase (controller)	dpo@edubase.net
You take an organization's exam, course or training, or your account was created by the organization	the organization (controller); EduBase works on its behalf and on its instructions (processor)	primarily the organization's data protection contact; we forward the request
You take an organization's exam, course or training, or your account was created by the organization	the organization (controller); EduBase works on its behalf and on its instructions (processor)	primarily the creator, whose name is shown on the start page or in the creator's own notice; we forward the request
Invoicing, account security, prevention of abuse (also in organizational use)	EduBase (controller)	dpo@edubase.net

[2.1.] When we process data on behalf of an organization, we act in accordance with Article 28 of the GDPR, on the basis of Chapter 8 of the GTC or a separate data processing agreement concluded with the organization.

- We do not use these data for our own purposes: marketing, newsletters, sending offers, profiling, sale or AI training.
- The organization informs you about the purpose, legal basis and retention period of the processing, for example through its own notice displayed on the exam start form.
- In this case, this Policy describes how we work as a processor: which subcontractors we use, where we store data and what security measures we apply.

We act in the same way if a user creates an exam without an organization and processes the data of other persons in it (creator). In this case, the provisions of this Policy relating to organizations also apply to the creator.

[2.2.] If you join an organization with your own EduBase account, EduBase remains the controller of your account's basic data. The controller of the activity carried out at the organization (results, progress, data requested by the organization) is the organization. The organization can see your results and the data you provided to it according to its settings, but not the other content of your account.

[3.] What data do we process, why and for how long?

The table lists the purposes for which EduBase decides as controller. The legal bases refer to Article 6(1) of the GDPR: (a) consent, (b) performance of a contract, (c) legal obligation, (f) legitimate interest.

Purpose	Data	Legal basis	Retention
Creating an account and providing the Service	full name, e-mail address, username, password (only as an encrypted hash), language, time zone, method and time of registration	(b)	until the account is deleted
Voluntary profile data	gender, date and place of birth, educational institution, year of graduation, profile picture	(a)	until deleted or until consent is withdrawn
Social login (Google, Microsoft, Facebook)	identifier received from the provider, name, e-mail address, profile picture	(b)	until the link is removed or the account is deleted
Phone number verification and SMS notifications	phone number, verification code	(a)	until deleted; the code until it expires
Own learning, quizzes, content creation	answers, results, activity (Chapter 4), uploaded content	(b)	until the account or the content is deleted
System notifications (e-mail, system message)	name, e-mail address, language, notification settings	(b)	until the account is deleted
Browser push notifications	device identifier (push token)	(a)	until unsubscribing

Newsletter and offers	name, e-mail address, language, time of subscription, opening of the newsletter	(a) (Section 6 of Grt.)	until unsubscribing
Purchase, invoicing	name or company name, billing address, tax number, e-mail address, order details, payment transaction identifier	(b), (c)	accounting documents for 8 years (Section 169 of Sztv.)
Contact, customer service, requests for quotation	name, e-mail address, phone number, company name, content of the message	(b), (f)	2 years from the closing of the case; correspondence related to a contract or to enforcing claims until the limitation period expires (generally 5 years)
Consumer complaints	the complaint and the response	(c) (Section 17/A of Act CLV of 1997 on consumer protection, Fgytv.)	the record of the complaint and the response for 3 years (Section 17/A(7) of Fgytv.)
Security, prevention of abuse	IP address, browser and device data, login times, failed logins, trusted devices, result of bot filtering	(f)	security logs for 5 years, certain error logs for 30 days; log extracts needed for a specific incident or legal dispute are kept separately until the case is closed, at most until the limitation period expires (5 years)
Usage statistics, development	page views, clicks, device type, approximate location (Chapter 8)	(a) consent in the cookie banner or in Cookie settings; (f) for anonymous aggregation	for the lifetime of the cookie, and at the provider for up to 14 months
Leaderboard	username, score; full name and profile picture only with the user's permission; on the leaderboard of competition exams, the full name, username and profile picture are always shown	(f), can be hidden in the settings; display of the full name: (a)	until the account is deleted or until hidden
Deletion of inactive accounts	e-mail address, last activity	(f)	warning after 360 days of inactivity (or if there is no login within 3 days of registration), then deletion after 14 days; does not apply to paid, organizational, API, SSO and LTI accounts
Legal claims, requests from authorities	the data concerned in the case	(c), (f)	until the limitation period expires (generally 5 years) or until the proceedings are closed with final effect

[3.1.] Without the mandatory data, the account cannot be created; the absence of voluntary data does not restrict the Service.

[3.2.] **Backups**. We keep the encrypted backups of the system for 16 months and then delete them automatically; this is how long it takes for the data of a deleted account to disappear from the backups as well. We access the backups only when restoring all or part of the system after a failure. In that case, as part of the restoration and before user access is reopened, we delete again, based on the deletion log, the accounts and data deleted since the backup was made. We do not restore data deleted at an individual's request from a backup. We keep an archive copy of deleted accounts and content for 90 days in order to restore them in the event of an erroneous deletion, and then delete it. If the deletion is carried out in response to a data protection request, no archive copy is made. We keep the fact of the deletion (identifier and time) together with the security logs for up to 5 years, as required for repeating the deletion when restoring backups.

[3.3.] **Legitimate interest**. Before processing based on legitimate interest, we carry out and document a balancing test: we examine the lawfulness of our interest, the necessity of the processing, and its impact on your interests and rights. We will send you the result of the balancing test upon request. The specific legitimate interests:

Purpose	Legitimate interest
Contact, customer service	answering inquiries and settling disputes

Security, prevention of abuse	protecting the Service and accounts against unauthorized access and attacks
Performance measurement, anonymous statistics	maintaining the speed and reliability of the Service
Exam security score in our own exams	protecting the integrity of exams
Leaderboard	motivating users and community game elements
Deletion of inactive accounts	deleting unnecessary data and data minimization
Legal claims	establishing, exercising and defending legal claims
Retaining the content of deleted accounts	the integrity of the Service: earlier exam results and other users' content may refer to them

[3.4.] Content uploaded under the free plan. We may incorporate content uploaded under the free plan into the shared content database of the Service in accordance with Section 10.6 of the GTC. Before incorporation, we remove personal data from the content, and we indicate the author's name only at their request. Deleting the account deletes the data relating to the author. Content already incorporated into the shared database that does not contain personal data is retained after the account is deleted. If the author is a Consumer and terminates the contract because of defective performance, failure to supply the service or a disadvantageous amendment, only the exceptions set out in Section 10.6 of the GTC are retained. Copies that other users incorporated into their own content before the deletion are retained with them, without personal data referring to the author.

When an account is deleted, we detach the content created by the user (for example questions, Quiz sets, exams, videos) from the account and deactivate it; it can then no longer be linked to the user. The purpose of retaining it is the integrity of the Service, because earlier exam results and other users' content may refer to it (legitimate interest, (f)). If such content contains personal data (for example a name, or a face in a video), we delete it upon request; the user may also delete it themselves before deleting the account.

[3.5.] E-mails. The retention periods in the table also apply to correspondence conducted by e-mail. We delete expired e-mails from the mailboxes on the basis of an automatic retention rule or a regular review carried out at least once a year. We store the delivery events of system notifications sent (for example delivered, bounced) for 180 days; the e-mail delivery provider deletes its own logs in accordance with its contract with us.

[4.] Exams, quizzes, learning data, exam security

The following data are generated during learning and examination. For an organizational exam, the controller of these data is the organization (Chapter 2); for your own practice, it is EduBase.

- **Answers and results**: the answers given, scores, grades, skill-level results, the grader's comments and the certificates issued.
- **Attempt data**: start and end time, time spent on questions, navigation between questions, other activity on the interface, the IP address and the type of device used.
- **Custom data**: fields requested by the creator of the exam on the exam start form (for example identifier, date of birth, class). The creator of the exam is responsible for their scope and legal basis.
- **Videos and learning materials**: the time and length of viewing, the sections viewed, and the fact that mandatory readings and documents have been read.
- **Training and competency records**: requirements completed, deadlines, attendance, uploaded certificates and evidence, and progress along the learning path (journey).

[4.1.] Exam security. To ensure fair examination, depending on the exam settings, we record the following events in the browser:

- leaving the exam window and exiting full-screen mode;

- the fact of copying and pasting (not the content of the clipboard);
- the rhythm and speed of typing (not the keys pressed);
- the fact that a screenshot was taken (not the image itself);
- when Safe Exam Browser is used, the browser and configuration verification key.

From these, the system calculates an indicative suspicion score between 0 and 100 on the basis of predefined, weighted rules, without an AI model or machine learning; the score is visible only to the organizer of the exam and authorized persons. A signal requires several independent factors to be present at the same time. The score is not evidence and does not entail any automatic consequence (Chapter 5). **We do not use cameras, microphones, screen recording or biometric identification.**

We have carried out a data protection impact assessment for exam security scoring, which covers false signals, the use of accessibility tools (for example dictation, screen readers) and the risk of misinterpreting the score. If the feature is used by an organization, carrying out the impact assessment is the organization's task; for this purpose, we will send our own assessment and a description of how the feature works upon request. The organizer may delete the score; the system does not recalculate a deleted score.

[4.2.] When an exam or quiz is taken without registration (exam code, public quiz), we link the above data to the name or identifier provided or to a random session identifier.

[4.3.] If the organization or the creator is the controller, they determine the retention period: they may delete the results at any time or export them to their own system. Deleting the exam also deletes the results belonging to it. If the creator deletes their account, we detach and deactivate the exam (Section 3.4). We then retain the candidates' results as controller ((b)) until the candidate's account is deleted or at the candidate's request. For your own practice, where EduBase is the controller, retention lasts until the account or the content is deleted. Temporary exam accounts generated by the organization are deleted after the exam is closed, in accordance with the organization's settings.

[5.] Artificial intelligence, profiling, automated decision-making

[5.1.] **AI features**. If you or your organization use an AI feature (generation of questions and learning material, translation, chat assistant, image generation, exam summary), we transfer the text, image or document needed for the task to the AI provider named in Chapter 6.

- The providers process the data via an API and do not use them for model training. For abuse monitoring, they may keep requests and responses for up to 30 days (requests flagged as suspected violations may be kept longer by the provider). Where possible, we switch off the storage of responses; we send the conversation history ourselves with each request. To prevent abuse, we also pass on a pseudonymized user identifier (not a name or e-mail address).
- We store the history of AI chats until the chat or the account is deleted.
- The exam summary receives only group-level data without names, from the results of at least 10 different participants; repeated attempts by the same person count as one person for the purposes of this threshold. Categories with fewer than 3 people are merged or sent only as a range, and individual extreme values (best, weakest result) are not sent. No names, e-mail addresses, suspicion scores or individual answers are transferred. Since in a small group the result may be traceable to individuals, we treat these data as personal data as well. Meeting the threshold does not in itself prove anonymity. If it cannot be reliably established that the participants are different persons, we do not transfer the data needed for the summary.
- We mark content created with AI on the interface and always indicate when you are talking to an AI assistant.
- The legal basis is the provision of the service ((b)); in organizational use, we act as a processor on the legal basis determined by the organization (Chapter 2).

[5.2.] Profiling. We automatically evaluate user data in the following cases:

Why?	What does it examine?	Legal basis
Learning support	calculating skill levels and weak points, recommending practice tasks, selecting the next step along the learning path according to the organization's rules	(b); in organizational use, the organization's legal basis (as processor)
Exam security	the suspicion score under Section 4.1	(f) for our own exams; for organizational exams, the organization's legal basis (as processor)
Marketing	grouping newsletter subscribers by interest (language, features used, plan)	(a)

You may object to profiling for marketing purposes at any time, or unsubscribe from the newsletter. We do not use data processed on behalf of an organization for marketing purposes.

[5.3.] Automated decision-making. EduBase does not, for its own purposes, take decisions concerning you based solely on automated processing that produce legal effects or similarly significant effects (Article 22 of the GDPR).

The organizer of an exam may set the system to automatically score, grade, issue certificates or route participants along the learning path. The organizer configures this according to the correct answers, scoring rules and grade boundaries they have specified.

If the automatic result produces legal effects or similarly significant effects – for example it results in an official grade, a professional qualification or exclusion from progression – the organizer may apply a solely automated decision only where an exception defined in Article 22 of the GDPR and the applicable safeguards are in place. Otherwise, the organizer must ensure meaningful human assessment before such an effect is produced. The person carrying out the assessment must actually evaluate the automatic result and the relevant circumstances of the case and must be authorized to change the result. A review that can only be requested afterwards does not in itself replace this prior human assessment.

The organizer informs the data subjects about the logic of the evaluation (scoring rules, grade boundaries) and its consequences, ensures that they can express their point of view, and that they can request human review. For this purpose, the system provides review requests, manual grading and re-evaluation. No adverse decision may be taken on the basis of the suspicion score without human assessment.

The automatic feedback of practice Quiz sets is for information only and does not qualify as an official evaluation.

[5.4.] Which features use AI? For transparency under the AI Act (Regulation (EU) 2024/1689), the following table shows where an AI system is at work and where it is not.

Feature	Uses AI?	What does the AI receive?	Who decides on the result?
Generation of questions and learning material, translation, title suggestions	yes	the text, image or document provided by the content creator	the content creator, who approves or rejects it
Image generation	yes	the description provided	the content creator; the image receives a machine-readable marking
Chat assistant in courses, quizzes, exams	yes	the user's messages and the background material provided by the organizer	the user; the assistant does not score, and its use may result in a point deduction according to the organizer's settings
Summary of exam results for the instructor	yes	group-level aggregated statistics without direct identifiers, with the restrictions under Section 5.1. If re-identification is possible, the data still qualify as personal data.	the instructor; no individual evaluation is produced

Automatic grading and grades	no; based on the correct answer and scoring rule specified by the question's creator	–	the organizer of the exam
Suspicion score	no; based on predefined, weighted rules	–	the organizer of the exam, with human assessment
Learning path (journey) and competency requirements	no; based on rules set by the organization	–	the organization

[5.5.] What we do not do with AI.

- We do not use emotion recognition, biometric identification or categorization, or manipulative techniques (Article 5 of the AI Act).
- We do not use AI to decide on admission or access, we do not evaluate individual learning or workplace performance, and we do not use AI to monitor the behavior of candidates (points 3 and 4 of Annex III to the AI Act).
- Under the GTC, organizations may not use the AI features for such purposes without a separate agreement.

[5.6.] Voluntary declaration on the use of AI. The organizer of an exam may ask you to declare at the end of the attempt whether you used AI. The answer is voluntary, refusing to answer has no consequences, and the answer is visible only to the organizer or authorized persons.

[5.7.] You can send your questions and comments about the AI features to dpo@edubase.net.

[6.] Processors and recipients

The “Role” column of the tables indicates whether the provider works as a processor on our instructions or acts as an independent or joint controller; the same company may have different roles for different operations. Data processed on behalf of organizations are handled only by the processors marked “Organization data”; they are the organization's sub-processors. The “Use” column indicates whether a service operates only depending on a setting, your choice or your consent. We publish changes to the list at least 15 days in advance, and we also inform organizational customers separately by e-mail or system notification.

[6.1.] Operation and infrastructure

Provider	Task	Data	Data location	Use	Role	Organization data
RamNode LLC (United States)	servers, database	data stored in the Service, uploaded files	Netherlands (EU)	always	processor	yes
Amazon Web Services EMEA SARL (Luxembourg)	hosting and cloud services: servers, file storage, encrypted backups, content delivery	data stored in the Service, backups, uploaded files	EU region	always	processor	yes
Cloudflare, Inc. (United States)	DNS, content delivery, attack protection, bot filtering (Turnstile), video hosting and playback, public libraries	IP address, request data, browser data	global network; DPF/SCC	always	processor	yes
Cloudflare, Inc. (United States) – Observatory / Web Analytics	measuring page load speed on real visits (RUM)	load times, page address, referring page, browser and device type, country; does not use cookies and does not identify the visitor	global; DPF/SCC	always; based on legitimate interest ((f))	processor	no
Mailgun Technologies, Inc. (United States)	sending system notification e-mails	name, e-mail address, content of the message, delivery data	EU region	always	processor	yes

Microsoft Ireland Operations Ltd. (Ireland)	customer service correspondence, backup e-mail sending (Microsoft 365)	name, e-mail address, content of the message	EU region	always, or depending on the setting	processor	yes
JW Player (Longtail Ad Solutions, Inc., United States)	video hosting and playback	IP address, playback data	global; DPF/ SCC	for uploaded videos	processor	yes
OneSignal, Inc. (United States)	browser push notifications	push token, internal user identifier, language	United States; DPF/ SCC	only after subscribing	processor	yes
Twilio Inc. (United States)	sending SMS (phone number verification, notifications)	phone number, text of the message	United States; DPF/ SCC	if the SMS feature is enabled	processor	yes
Superblock LLC – Pushover (United States)	push notifications (with the Pushover app)	typically contains no personal data	United States	depending on the setting	processor	no

[6.2.] Payment and invoicing

Provider	Task	Data	Data location	Use	Role	Organization data
Billingo Technologies Zrt. (Hungary)	issuing invoices and payment requests, reporting to the Hungarian Tax Authority (NAV)	billing data (name or company name, address, tax number, e-mail address, items, amount)	EU	when purchasing (main invoicing provider)	processor	no
OTP Mobil Kft. – SimplePay (Hungary)	bank card payment	name, e-mail address, billing data, amount; card data are seen only by the provider	EU	if you choose this payment method	independent controller	no
PayPal (Europe) S.à r.l. et Cie, S.C.A. (Luxembourg)	payment	name, e-mail address, amount, transaction data	EU	if you choose this payment method	independent controller	no
Stripe Payments Europe, Ltd. (Ireland)	bank card and other online payment, invoicing, fraud prevention	name, e-mail address, billing data, amount, IP address, device data; card data are seen only by the provider	EU/ global; DPF/SCC	if you choose this payment method	independent controller (payment, fraud prevention); processor (invoicing)	no
N-Ware Kft. (Hungary)	issuing invoices, reporting to the Hungarian Tax Authority (NAV)	billing data	EU	when purchasing (if configured)	processor	no
Paymentwall, Inc. (United States)	alternative payment	name, e-mail address, amount	United States; DPF/SCC	if you choose this payment method	independent controller	no

OTP Bank Nyrt. and Wise Europe SA (Belgium), which receive bank transfers, process the payer's name, account number and the payment reference as independent controllers in accordance with payment services legislation. If you transfer in USD, the bank you have chosen forwards the payment order to Wise's US partner bank, Community Federal Savings Bank (New York); this data flow is carried out by the payment service providers as independent controllers, not by EduBase.

[6.3.] Login, AI and content features

Provider	Task	Data	Data location	Use	Role	Organization data
Google Ireland Ltd. (Ireland)	Google login, importing the profile picture	Google identifier, name, e-mail address, profile picture	EU/global; DPF/SCC	if you choose it	independent controller	no
Microsoft Ireland Operations Ltd. (Ireland)	Microsoft login (Entra ID), importing the profile picture	Microsoft identifier, name, e-mail address, profile picture	EU/global; DPF/SCC	if you or your organization choose it	independent controller	no

Meta Platforms Ireland Ltd. (Ireland)	Facebook login	Facebook identifier, name, e-mail address, profile picture	EU/global; DPF/SCC	if you choose it	independent controller	no
Automattic Inc. – Gravatar (United States)	retrieving the profile picture, only at the user's request (“Use Gravatar image”)	a hash generated from the e-mail address; this is not encryption and is not necessarily anonymous	United States; DPF/SCC	at the user's request	independent controller	no
OpenAI (OpenAI Ireland Ltd. / OpenAI, L.L.C.)	AI features, moderation of AI content	the text, image or document provided for the task	United States; DPF/SCC	when using an AI feature	processor	yes
Anthropic (Anthropic Ireland Ltd. / Anthropic, PBC)	AI features	the text, image or document provided for the task	United States; DPF/SCC	when using an AI feature	processor	yes
Google Cloud EMEA Ltd. – Vertex AI Gemini (Ireland)	AI features	the text, image or document provided for the task	EU region	when using an AI feature	processor	yes
Amazon Web Services EMEA SARL – Amazon Bedrock (Luxembourg)	AI features (with the models available on Bedrock)	the text, image or document provided for the task	EU region	when using an AI feature	processor	yes
Fonticons, Inc. – Font Awesome (United States)	loading the icon set	IP address, browser data	United States; DPF/SCC	depending on the configuration	independent controller	no
Google Ireland Ltd. – Google Fonts	loading fonts	IP address, browser data	global; DPF/SCC	depending on the configuration	independent controller	no

[6.4.] Statistics and marketing (only with consent, Chapter 8)

Provider	Task	Data	Data location	Use	Role	Organization data
Google Ireland Ltd. – Google Analytics, Tag Manager	visitor statistics	cookie identifier, page views, device data, a pseudonymized identifier for logged-in users	EU/global; DPF/SCC	with consent	processor	no
Hotjar Ltd. (Malta)	usability analysis (heatmaps, session replay; typed text is hidden)	cookie identifier, clicks, device data	EU	with consent	processor	no
Meta Platforms Ireland Ltd. – Meta Pixel, Messenger chat	advertising measurement, chat	cookie identifier, page views, content of the chat	EU/global; DPF/SCC	with consent	joint controller (Pixel), independent controller (Messenger)	no
The Rocket Science Group LLC – Mailchimp (United States)	business newsletter for organizational contacts	e-mail address, language	United States; DPF/SCC	when subscribing	processor	no
SolarWinds – Pingdom RUM (United States)	measuring page load speed	IP address, load times	United States	with consent	processor	no

The meaning of the abbreviation “DPF/SCC” is explained in Chapter 7.

[6.5.] **Embedded external content**. If learning material embeds YouTube, Vimeo, GeoGebra, Prezi or other external content, your browser connects directly to the external provider during playback. In this case, the provider acts as an independent controller, in accordance with its own notice.

[6.6.] **Integrations chosen by the organization**. The organization may transfer the data to its own systems or load them from there. Examples of such integrations are LTI (for example Moodle, Canvas), SSO and LDAP, webhooks, the API and MCP, and HR and school systems (for example Nexon, Wonde). In these cases, the organization decides and is responsible for the system it has chosen.

[6.7.] **Other recipients**. We disclose data to authorities, courts and law enforcement agencies only on a legal basis, after examining the lawfulness of the request; for organizational data, we also inform the organization of this unless prohibited by law. Our legal counsel, accountant and auditor may access the data necessary for their tasks, subject to confidentiality. We do not sell personal data.

[7.] Transfers to third countries

[7.1.] We store the primary application database and our own backups exclusively in the European Union: on RamNode's servers in the Netherlands and in the European regions of Amazon Web Services (Frankfurt, Ireland). Certain external providers (for example AI providers, the content delivery network, the push and SMS providers) may also process or temporarily store data outside the EU, as shown in the "Data location" column in Chapter 6; remote access by US parent companies is also possible. The safeguards under Section 7.2 apply to these.

[7.2.] Transfers outside the European Economic Area take place only with safeguards under Chapter V of the GDPR:

- an **adequacy decision**, for example for the United Kingdom, or for US companies that have joined the EU–US **Data Privacy Framework** (**DPF**);
- **standard contractual clauses** adopted by the European Commission (**SCC**), with supplementary measures (for example encryption, data-minimizing transfers), if the recipient has not joined the DPF.

[7.3.] We do not transfer data to a country for which there is neither an adequacy decision nor appropriate safeguards.

[7.4.] You can request a copy of the documents evidencing the transfer safeguards at dpo@edubase.net.

[8.] Cookies and similar technologies

[8.1.] A cookie is a small data packet that a website stores in your browser. We also use the browser's local storage (localStorage or sessionStorage) for similar purposes. Strictly necessary cookies do not require consent; functional, statistics and marketing cookies are loaded only with the consent you give per category (Section 155(4) of the Hungarian Act on electronic communications).

[8.2.] **How consent works**.

- **Categories**. We group non-essential cookies into three categories: functional (for example Meta/Facebook integrations and Messenger chat, OneSignal browser notifications), statistics (for example Google Analytics, Google Tag Manager, Hotjar) and marketing (for example Meta Pixel). All three are switched off by default and are switched on only after your express decision.
- **Visitors who are not logged in** can decide per category in the cookie banner displayed on their first visit. The "Accept all" and "Reject all" buttons have equal prominence.
- **Registered users** decide separately, per category and voluntarily. Registration and accepting the GTC and this Policy do not constitute consent to cookies. Until they have decided, the cookie banner is displayed even when logged in, and no non-essential cookie is loaded until then. We store the decision and its time linked to their account, and log changes to demonstrate consent.
- **Withdrawal and modification**. Consent can be withdrawn or modified at any time as easily as it was given: with the "Cookie settings" link at the bottom of every page, when logged in under My account → Settings → Cookie settings, or at dpo@edubase.net. Withdrawal takes effect immediately: the page reloads and the services concerned are no longer loaded. Withdrawal does not affect the lawfulness of earlier processing.
- Cookies (including cookies previously placed by external providers) can be deleted and blocked in your browser settings, but login does not work without the cookies necessary for operation.

[8.3.] Strictly necessary cookies (our own)

Name	Purpose	Lifetime
[prefix]_session (for example edubase_session)	identifying the session	until the end of the session
[prefix]_user (for example edubase_user)	logging in again a user who chose to stay logged in (encrypted)	30 days
[prefix]_authenticator… (for example edubase_authenticator_…)	remembering a device marked as trusted for two-factor authentication (encrypted)	180 days
[prefix]_cookies (for example edubase_cookies)	checking whether the browser allows cookies	until the end of the session
[prefix]_lti (for example edubase_lti)	operation of the LTI integration (Moodle, Canvas) in an embedded view	until the end of the session
CloudFront-Policy, **CloudFront-Signature**, **CloudFront-Key-Pair-Id**	authorization check for protected videos and files	until access expires
__cf_bm, **cf_clearance**	attack protection, bot filtering (Cloudflare)	30 minutes – 1 year

For visitors who are not logged in, we store the decision made in the cookie banner in the browser (**cc_cookie**, 6 months) and in the session; for logged-in users, in their account. In this case, the browser's local storage ([prefix]_cookie_consent) only holds a copy of the decision stored in the account.

[8.4.] Statistics, functional and marketing cookies (with consent)

Category	Provider	Typical names	Purpose	Lifetime
statistics	Google Analytics, Tag Manager	_ga, _ga_…	visitor statistics	13 months
statistics	Hotjar	_hjSessionUser_…, _hjSession_…	usability analysis	30 minutes – 1 year
marketing	Meta Pixel	_fbp	advertising measurement	3 months
functional	Meta Messenger chat	Meta cookies	customer service chat (functional)	according to Meta's rules
functional	Facebook SDK	Meta cookies on the facebook.com domain (for example fr); the SDK does not place cookies on the website's own domain	Facebook integrations: loading social plugins (for example the Like button)	according to Meta's rules
functional	OneSignal	localStorage, IndexedDB	managing push subscriptions	until unsubscribing

Google Tag Manager and Google Analytics are loaded only with statistics consent, and only tags for statistical purposes run in Google Tag Manager. Google tags also receive the consent signals (Google Consent Mode): we allow storage and data use for advertising purposes (**ad_storage**, **ad_user_data**, **ad_personalization**) only with marketing consent.

[8.5.] The exact list of external providers' cookies may change over time; the current list is included in the notice of the provider concerned.

[9.] Data security and personal data breaches

[9.1.] In accordance with Article 32 of the GDPR, we apply technical and organizational measures proportionate to the risk. The most important are:

- **Encryption**: all connections run over HTTPS (TLS). We store passwords only as one-way hashes, and we encrypt login cookies and backups.
- **Access protection**: we apply a password policy, lockout after repeated failed logins, two-factor authentication, bot filtering, CSRF protection and API rate limiting.
- **Permission management and separation**: we use role-based permissions. The data of organizations are logically separated from one another, and protected videos and files can only be accessed through signed, expiring links.
- **Logging**: we log logins, administrative operations and errors.
- **Availability**: we make regular, encrypted backups to EU data centers and use attack protection.
- **Staff**: only staff bound by confidentiality have access to the data, to the extent necessary for their tasks. Administrator access requires two-factor authentication.
- **Development**: we install security updates regularly, and changes are checked by automated tests.

[9.2.] **Incidents**.

- We keep a record of personal data breaches.
- If a breach involves a risk, we notify the NAIH within 72 hours of becoming aware of it.
- If it involves a high risk, we also inform the data subjects without undue delay.
- If the breach affects data processed on behalf of an organization, we notify the organization without undue delay and at the latest within 48 hours, or within any shorter deadline undertaken in our contract with it. In this case, the organization decides on the notification to the authority and on informing the data subjects.

[9.3.] You can report a security vulnerability or suspicious event at webmaster@edubase.net. We are grateful for good-faith, responsible vulnerability reports and will not take legal action against them.

[10.] Your rights, remedies, minors

[10.1.] You may exercise the following rights. We fulfill requests without undue delay and at the latest within one month; where justified, this may be extended by two months, in which case we will inform you.

Right	What does it mean?
Access (Article 15)	information about which of your data we process, and a free copy of them (XLSX)
Rectification (Article 16)	correcting inaccurate data; most data can also be changed by yourself in the account settings
Erasure (Article 17)	deleting the account and the data, if there is no statutory retention obligation
Restriction (Article 18)	suspending the processing for the duration of a dispute or verification
Data portability (Article 20)	the data you provided in a machine-readable format or, on request, directly to another controller
Objection (Article 21)	against processing based on legitimate interest and against profiling for marketing purposes; unconditionally in the case of marketing
Withdrawal of consent (Article 7)	at any time, without affecting the lawfulness of earlier processing
Human review (Article 22)	for automated evaluation: expressing your point of view, human review and learning the logic of the decision; can be requested from the organizer of the exam or with the system's review request (Section 5.3)

[10.2.] **How can you make a request?** Write to dpo@edubase.net or use the data protection category of the Contact form. You can unsubscribe from the newsletter with the link in the e-mails, and from push notifications in your browser. The easiest way to identify yourself is to write from the e-mail address associated with your account, or to use the Contact form while logged in. If this is not possible, we will identify you in another proportionate way (for example with questions about your account data); we only ask for the data necessary for identification. Fulfilling the request is free of charge; for manifestly unfounded or excessive requests, we may charge a reasonable fee or refuse the request.

[10.3.] **Organizational data**. If your data are processed on behalf of an organization (Chapter 2), we forward your request to the organization and help it to fulfill it. It is faster if you contact the organization directly.

[10.4.] **Remedies**.

- You can lodge a complaint with the Hungarian National Authority for Data Protection and Freedom of Information (NAIH): 1055 Budapest, Falk Miksa utca 9–11., Hungary; postal address: 1363 Budapest, Pf. 9.; phone: +36 1 391 1400; e-mail: ugyfelszolgalat@naih.hu; www.naih.hu.
- You can also lodge a complaint with the supervisory authority of the EU Member State of your habitual residence or place of work.
- You can also go to court; you may also bring the action before the regional court of your place of residence or stay.
- We recommend that you contact us first so that we can resolve the matter quickly.

[10.5.] **Minors**.

- For self-registration, processing based on consent concerning a user under the age of 16 – for example voluntary profile data and optional cookies – requires the consent or authorization of the legal representative holding parental responsibility (Article 8 of the GDPR, Section 6 of Infotv.). We ask for a separate declaration on this at registration, record it together with its time and, where justified, ask for the consent to be presented; a template for the declaration is provided on the Website. Processing necessary for the performance of the contract takes place on a separate legal basis, provided that the contract has been validly concluded.
- If the account is created or managed by a school, the school is the controller; the school takes care of the legal basis and of informing parents.
- We do not use the data of minors for marketing purposes or for profiling for marketing purposes; the learning-support skill profile and the exam security score under Section 5.2 also apply to them.
- Users under 18 (based on the date of birth provided) are not shown on the global leaderboard by default (the leaderboard of competition exams is managed by the organizer of the exam). If they themselves ask to appear, only their username is shown.
- If we become aware that the necessary parental consent or authorization is missing, we stop the processing based on it. We delete such data without undue delay, unless there is a separate legal basis for retaining certain data; in that case we provide separate information about the purpose and duration. The absence of consent does not affect processing lawfully carried out on a different, valid legal basis.

[11.] Amendment and entry into force

[11.1.] We update this Policy when legislation, the Service or the providers we use change. We publish any material change on the Website at least 15 days before it applies, and within the same period we also inform the affected registered users by e-mail. The notice sets out the change, the date from which it applies, and the choices and rights available to the data subjects. The system notification displayed at login supplements this. An amendment of this Policy and the notice sent about it do not in themselves constitute consent to new processing.

[11.2.] If we wish to use personal data for a new purpose not covered by this Policy, we will inform you in advance and, if the legal basis is consent, ask for separate consent.

[11.3.] Earlier versions are available on the Website.

[11.4.] This Policy enters into force on 1st December 2026.