

Privacy Policy

English-language version

PRIVACY POLICY

EN

How **QUASAR.HUB** processes personal data of Clients, Participants, business Clients, job candidates, employees, associates and contractors – purposes, legal bases, retention periods and data-subject rights.

CONTROLLER

QUASAR.HUB sp. z o.o.

REGISTERED OFFICE

os. Stefana Batorego 79E/1, Poznań

EFFECTIVE FROM

10 September 2026

PRIVACY CONTACT

privacy@quasarhub.pl · +48 579 135 924

Spis treści

Privacy Policy (EN) · QUASAR.HUB sp. z o.o.

- I.** General provisions
- II.** Definitions
- III.** Scope of application
- IV.** Purposes and legal bases of processing
- V.** Categories of data processed
- VI.** Retention periods
- VII.** Cookies and similar technologies
- VIII.** Profiling and marketing
- IX.** Recipients of data and transfers outside the EEA
- X.** Principles of processing and rights of data subjects
- XI.** Protection of minors' data
- XII.** Security measures
- XIII.** Contact
- XIV.** Final provisions

I. General provisions

1. This Privacy Policy (the "**Policy**") sets out the rules for processing personal data of Clients, Participants, business Clients and their employees and associates, job candidates, employees, associates, contractors, and users of the website and Platform of **QUASAR.HUB sp. z o.o.** (the "**Controller**" or "**School**"), which provides language courses and interest-development courses (including STEM subjects) in individual and group formats, on site and online, makes a self-study Space available to Participants, and runs group courses for the employees of business clients.
 2. The Policy is based on Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**GDPR**"). The Controller applies appropriate technical and organisational measures to protect the personal data it processes.
 3. "Personal data" means any information relating to an identified or identifiable natural person – one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier.
 4. **The School admits only persons who have reached the age of 15. Contracts are concluded exclusively by adults.** Participants therefore include persons aged 15–17, whose data are processed with particular care – see Section XI.
-

II. Definitions

1. **Controller** – QUASAR.HUB sp. z o.o., with its registered office at os. Stefana Batorego 79E/1, 60-687 Poznań, Poland, entered in the Register of Entrepreneurs of the National Court Register under number **KRS 0001265147**, NIP **9721383160**, REGON **545663419**, share capital **PLN 6,000.00**, registry court: District Court Poznań – Nowe Miasto i Wilda in Poznań, 8th Commercial Division of the National Court Register.
2. **Client** – an adult with full legal capacity who enters into an agreement with the Controller for the provision of educational services, on their own behalf or on behalf of a Participant, including via the Website, e-mail or telephone.
3. **Participant** – a person enrolled in a course run by the School or using the Space; this may be a person aged 15–17 enrolled by a Guardian, or an adult enrolling themselves.
4. **Guardian** – a parent or legal guardian of a Participant under 18 years of age.
5. **Business Client** – an entrepreneur entering into an agreement with the Controller for the provision of services for its employees or associates.
6. **Employee/Associate of a Business Client** – a person registered by a Business Client to take part in classes organised for its staff.
7. **Job Candidate** – a person applying for employment or cooperation with the School, including as a teacher or instructor, regardless of the intended legal basis of cooperation.
8. **Employee** – a person employed by the Controller under a contract of employment.
9. **Associate** – a person cooperating with the Controller under a civil-law contract (contract of mandate, contract for specific work) or a B2B contract, including teachers and instructors.
10. **Contractor** – an entrepreneur cooperating with the Controller under a contract related to its business activity (e.g. a provider of accounting, hosting or marketing services).

- 11. Platform / Client Account** – a panel accessible after logging in on the Website, through which a Participant or Client can access course materials, the class schedule and, where introduced, the School's participant rewards system.
- 12. Space** – the open self-study area at the School's premises, made available to Participants outside class hours.
- 13. Website** – the website operated by the Controller at **quasarhub.pl**.
- 14. Cookies** – small text files stored on the user's device when visiting the Website; details are set out in the **Cookie Policy**, referred to in Section VII.
- 15. CSS (Child Safeguarding Standards)** – the *Standardy Ochrony Młodzieży* in force at the Controller.

III. Scope of application

This Policy applies to the Controller's processing of personal data of:

- Clients and Participants;
- Business Clients and their employees/associates registered for group courses;
- Job Candidates;
- the Controller's Employees;
- the Controller's Associates (including teachers and instructors);
- the Controller's Contractors and persons designated by them for contact;
- users of the Platform/Client Account and visitors to the Website;
- persons using the Space.

IV. Purposes and legal bases of processing

1. Clients and Participants

- 1.1.** Conclusion and performance of the agreement for educational services, including enrolling a Participant, issuing login credentials for the Platform and the online class platform, sending materials and recording attendance – **Art. 6(1)(b) GDPR**. This concerns data of both the Client (usually the Guardian) and the Participant.
- 1.2.** Day-to-day course administration (change of group, notice of schedule changes, handling requests) – **Art. 6(1)(b) GDPR**.
- 1.3.** Running online classes via the video-conferencing platform and the Platform, including **recording classes solely on the basis of separate, voluntary consent** of the Participant or their Guardian – **Art. 6(1)(a) GDPR**. Consent is voluntary; withholding or withdrawing it does not prevent participation. Recordings are kept for no longer than **3 months**, unless they constitute evidence in pending proceedings – in which case until those proceedings are finally concluded.

- 1.4. **Capturing and publishing a Participant's image** (photographs, video and audio recordings from classes, events and competitions) in the School's promotional and documentation materials – **Art. 6(1)(a) GDPR** (consent); for a Participant under 18, written consent of the Guardian, and for a Participant who has reached 16, the School additionally obtains the Participant's own consent. Consent is voluntary, does not affect access to the School's offering, and may be withdrawn at any time. Detailed rules on protecting minors' images are set out in Section 14 of the CSS.
- 1.5. Direct marketing of the School's own services (new courses, promotions, the referral programme) by e-mail, SMS or telephone – **Art. 6(1)(a) GDPR** (consent), in conjunction with **Article 398 of the Act of 12 July 2024 – Electronic Communications Law**, which requires the recipient's prior consent for sending commercial information using telecommunications terminal equipment. Consent may be withdrawn at any time, including via the unsubscribe link.
- 1.6. Operating the newsletter – **Art. 6(1)(a) GDPR** (consent given on sign-up), in conjunction with Article 398 of the Electronic Communications Law.
- 1.7. Handling enquiries and trial-lesson bookings submitted through forms on the Website – **Art. 6(1)(b) GDPR** (steps prior to entering into a contract) or **Art. 6(1)(f) GDPR** (legitimate interest in responding), depending on content.
- 1.8. Compliance with the legal obligation arising from the **Act of 13 May 2016 on Counteracting Sexual Offences and Protecting Minors (consolidated text: Journal of Laws 2026, item 110)** – the Controller is an organiser of activities involving minors and has implemented Child Safeguarding Standards. Under CSS procedures, data of Participants who are minors and of their Guardians may be processed, including, in exceptional situations, special categories of data (e.g. health data) – **Art. 6(1)(c) and Art. 9(2)(b) and (g) GDPR** in conjunction with that Act.
- 1.9. Handling complaints and establishing, exercising or defending legal claims – **Art. 6(1)(b) and (f) GDPR**.
- 1.10. Compliance with tax and accounting obligations, including invoicing – **Art. 6(1)(c) GDPR**.
- 1.11. Operating the referral programme – to award and settle discounts for both the referrer and the referred person – **Art. 6(1)(b) GDPR**.
- 1.12. Ensuring the safety of persons using the Space and of the Controller's property – **Art. 6(1)(f) GDPR**. *(If the Controller operates CCTV at its premises, information on its scope, recording retention period and signage will be added here and displayed at the entrance. As at the effective date of this Policy, the Controller does not / does operate CCTV – to be confirmed before publication.)*
- 1.13. Keeping a record of entries to and exits from the Space by Participants (name, surname, date, time of entry and exit) – **Art. 6(1)(c) GDPR** in connection with the obligation to ensure the safety of minors under the Act on Protecting Minors, and **Art. 6(1)(f) GDPR**. The record is kept for **12 months** and made available to a Guardian on request with respect to their own child. The rules are set out in Section 8.6.5 of the CSS.

2. Business Clients and their employees/associates

- 2.1. Establishing cooperation and pre-contractual negotiations – **Art. 6(1)(b) and (f) GDPR**.

- 2.2. Conclusion and performance of the agreement for corporate services, including registering the Business Client's employees/associates, issuing login credentials and providing materials – **Art. 6(1)(b) GDPR** (towards the Business Client) and **Art. 6(1)(f) GDPR** (towards registered individuals and designated contact persons).
- 2.3. Producing attendance and progress reports delivered to the Business Client – **Art. 6(1)(f) GDPR**, to the extent agreed in the contract. The Controller does not disclose to the Business Client private information obtained during classes.
- 2.4. Invoicing and payment settlement – **Art. 6(1)(c) and (b) GDPR**.
- 2.5. Handling complaints and pursuing claims – **Art. 6(1)(f) GDPR**.
- 2.6. If a person under 18 takes part in corporate classes, Section IV.1.8 and the CSS apply accordingly.

3. Job Candidates

- 3.1. Conducting the recruitment process within the scope of data listed in Art. 22¹ § 1 of the Polish Labour Code – **Art. 6(1)(c) GDPR**; for civil-law or B2B cooperation – **Art. 6(1)(b) GDPR**.
- 3.2. Conducting recruitment with respect to data provided voluntarily beyond that scope (e.g. additional qualifications, portfolio) – **Art. 6(1)(a) GDPR**.
- 3.3. Assessing the candidate's skills and aptitude (trial lesson, qualification test) – **Art. 6(1)(f) GDPR**.
- 3.4. Considering the candidate in future recruitment processes – only on separate consent – **Art. 6(1)(a) GDPR**, for **12 months** from the date consent was given or until it is withdrawn, whichever is earlier.
- 3.5. Where the role involves contact with minors, the Controller – fulfilling the obligation under **Article 21 of the Act on Protecting Minors** – checks the candidate in the **Register of Sexual Offenders**, obtains information from the **National Criminal Register**, and, for persons who have resided outside Poland at any time in the last 20 years, obtains criminal-record information from the relevant country or a corresponding statutory declaration, together with the candidate's own declarations – **Art. 6(1)(c) GDPR**. Without a positive outcome, the candidate is not admitted to work with minors. Details are set out in Annex 4 to the CSS.

4. Employees

- 4.1. Work organisation and management, including personnel files – **Art. 6(1)(c) and Art. 9(2)(b) GDPR** in conjunction with the Labour Code, for the duration of employment and 10 or 50 years thereafter as applicable.
- 4.2. Payroll calculation and payment, including deductions – **Art. 6(1)(c) GDPR**.
- 4.3. Social-insurance, tax and accounting obligations – **Art. 6(1)(c) GDPR**.
- 4.4. Occupational health and safety obligations – **Art. 6(1)(c) and Art. 9(2)(b) GDPR**, for 10 years after the end of employment.
- 4.5. Compliance with Article 21 of the Act on Protecting Minors – as in Section IV.3.5 – **Art. 6(1)(c) GDPR**, for Employees having contact with minors.

- 4.6. On separate, voluntary consent – recording online classes or training sessions and using images in the School's promotional materials – **Art. 6(1)(a) GDPR**, until consent is withdrawn.
- 4.7. Pursuing and defending against claims – **Art. 6(1)(f) GDPR**, for 3 years after the end of employment, or until pending proceedings are finally concluded.

5. Associates (including teachers under civil-law and B2B contracts)

- 5.1. Conclusion and performance of the civil-law or B2B contract – **Art. 6(1)(b) and (c) GDPR**.
- 5.2. Remuneration, tax and accounting settlements – **Art. 6(1)(c) GDPR**.
- 5.3. Compliance with Article 21 of the Act on Protecting Minors, as in Section IV.4.5 – applies to every Associate having contact with minors, regardless of the basis of cooperation.
- 5.4. On separate, voluntary consent – recording classes and using images in promotional materials – **Art. 6(1)(a) GDPR**.
- 5.5. Pursuing and defending against claims – **Art. 6(1)(f) GDPR**.

6. Users of the Platform/Client Account and the Website

- 6.1. Maintaining a Platform account (name, surname, e-mail address, telephone number) and providing course materials and the schedule – **Art. 6(1)(b) GDPR**.
- 6.2. Ensuring the correct operation, continuity and security of the Website and Platform, including login authentication – **Art. 6(1)(b) and (f) GDPR**.
- 6.3. Website traffic analysis and measuring the effectiveness of marketing activities using analytics and marketing Cookies – **Art. 6(1)(a) GDPR** (consent given through the cookie banner), in conjunction with **Article 399 of the Electronic Communications Law**.
- 6.4. If the School introduces a participant rewards or points system, visibility of a Participant's results to other users requires **separate, voluntary consent** from the minor's Guardian (or from the Participant, if an adult) – **Art. 6(1)(a) GDPR**. Where visible to others, the Controller limits disclosure to the Participant's first name and the first letter of the surname, and shows only positive information (points earned, participation), never negative information (e.g. absences).

7. Contractors

- 7.1. Establishing and performing cooperation with suppliers of services to the School – **Art. 6(1)(b), (c) and (f) GDPR**.
- 7.2. Compliance with tax obligations related to the cooperation – **Art. 6(1)(c) GDPR**.
- 7.3. Pursuing claims and rights – **Art. 6(1)(f) GDPR**.

V. Categories of data processed

Depending on the relationship with the Controller, the following categories may be processed:

- identification and contact data (name and surname, date of birth, PESEL or another identification number where required by law, address, e-mail address, telephone number);
- data of a Participant's Guardian, including data confirming the right to represent the minor;
- data necessary to perform the agreement (course chosen, group, level, attendance, progress, test and exam results);
- payment data (bank account number or payment-card token processed by an external payment operator; the Controller does not store full card numbers);
- image and voice data (photographs, video and audio recordings from classes – only on the basis of separate consent);
- data submitted in a contact-form message or in correspondence;
- technical and website-usage data (IP address, device and browser type, pages visited, cookie identifiers);
- data relating to employment or cooperation (CV, references, qualifications, certificates, bank account number, tax and social-insurance data and, where relevant, health data connected with sick leave);
- for persons working with minors – criminal-record information and declarations required by the Act on Protecting Minors;
- in CSS procedures – data relating to the incident, in exceptional situations including special categories of data.

VI. Retention periods

CATEGORY	PERIOD
Data from the agreement with a Client/Participant	duration of the agreement + the limitation period for claims (as a rule 6 years; for the Controller's business-related claims – 3 years)
Data on invoices and accounting documents	5 years from the end of the calendar year in which the tax became due
Data processed on the basis of consent (marketing, newsletter, images)	until consent is withdrawn
Class recordings (IV.1.3, IV.4.6, IV.5.4)	max. 3 months ; if they constitute evidence in proceedings – until those are finally concluded, then permanently deleted
Recruitment data	duration of the recruitment process; with consent for future recruitment – 12 months from the date consent was given, or until withdrawal
Space entry/exit record	12 months from the date of entry
Article 21 verification records	duration of cooperation + the limitation period for claims
CSS procedure records (intervention record, support plan)	until the matter is closed; if referred to authorities – until those proceedings are finally concluded
Employee and Associate data	periods required by labour, tax and social-insurance law

CATEGORY	PERIOD
Analytics and marketing Cookies	periods indicated in the Cookie Policy, in any event no longer than 24 months , unless consent is withdrawn earlier
Data processed on the basis of legitimate interest	until an effective objection is raised

The Controller reviews the continued usefulness of the data it processes at least once every 3 years.

VII. Cookies and similar technologies

1. The Website uses Cookies and similar technologies (including local storage and pixels).
2. Four categories of Cookies are used: **necessary, analytics, marketing and functional**. Cookies other than necessary ones are used only after obtaining the user's consent, given through the cookie banner – **Article 399 of the Electronic Communications Law** in conjunction with Art. 6(1)(a) GDPR.
3. A detailed list of categories, purposes, example tools and storage periods is set out in the **Cookie Policy** available on the Website.
4. Consent may be withdrawn at any time through the cookie settings on the Website, without affecting the lawfulness of processing carried out before withdrawal.

VIII. Profiling and marketing

1. The Controller does not carry out automated decision-making, including profiling, producing legal effects concerning data subjects or similarly significantly affecting them.
2. Within direct marketing, the Controller may apply basic segmentation of newsletter recipients (e.g. by course type of interest) in order to send more relevant commercial information. The legal basis is consent – **Art. 6(1)(a) GDPR**. Consent may be withdrawn at any time.
3. If the Controller extends the scope of profiling in future (e.g. course recommendations based on Platform activity), the relevant information and legal basis will be set out in an updated version of this Policy **before** such processing begins.

IX. Recipients of data and transfers outside the EEA

1. Personal data may be disclosed to processors acting on the Controller's instructions under data-processing agreements, in particular:
 - the hosting provider for the Website and Platform;
 - the provider of the video-conferencing platform used for online classes;
 - the accounting office;

- the online payment operator;
 - providers of e-mail marketing, CRM and analytics tools;
 - the law firm;
 - the marketing agency – to the extent necessary.
2. Data may be disclosed to teachers and other staff to the extent necessary to run classes, and to public authorities where required by law – in particular the Police, the prosecutor's office, the family court or a social welfare centre in the course of an intervention under the CSS, as well as tax authorities and courts.
 3. Data of Participants registered by a Business Client may be disclosed to that Client within the reports referred to in Section IV.2.3.
 4. If any tool used by the Controller is supplied by an entity established outside the European Economic Area (e.g. in the United States), data may be transferred to a third country. In such cases the Controller uses only suppliers ensuring an adequate level of protection – on the basis of a European Commission adequacy decision, standard contractual clauses approved by the European Commission, or – for US suppliers – participation in the **EU-U.S. Data Privacy Framework**.
 5. A current list of tools used, together with the applicable transfer mechanism, is available on request at the address given in Section XIII.
-

X. Principles of processing and rights of data subjects

1. The Controller processes personal data lawfully, fairly and transparently, for specified and legitimate purposes, to an extent adequate to those purposes, keeping data accurate, limiting the storage period, and applying appropriate technical and organisational measures.
 2. Every data subject has the right to:
 - access their data and obtain a copy (Art. 15 GDPR);
 - rectify inaccurate or incomplete data (Art. 16 GDPR);
 - erasure (Art. 17 GDPR);
 - restriction of processing (Art. 18 GDPR);
 - data portability, for data processed by automated means on the basis of consent or contract (Art. 20 GDPR);
 - object to processing based on legitimate interest, including direct marketing (Art. 21 GDPR);
 - withdraw consent at any time, without affecting the lawfulness of processing carried out before withdrawal;
 - lodge a complaint with the **President of the Personal Data Protection Office** (Prezes Urzędu Ochrony Danych Osobowych), ul. Stawki 2, 00-193 Warsaw, or with the supervisory authority of the EU/EEA member state of their habitual residence.
 3. For a Participant under 18, these rights are exercised by their Guardian. A Participant who has reached 16 may independently withdraw consent to the use of their image (Section IV.1.4).
 4. Providing personal data is voluntary, but for Clients, Participants, Business Clients, Employees, Associates and Contractors it is a condition of concluding and performing the relevant agreement – refusal makes performance impossible. For Job Candidates, providing the data listed in Art. 22¹ § 1 of the Labour Code is a condition of taking part in recruitment.
-

XI. Protection of minors' data

1. A significant proportion of Participants are aged 15–17. The Controller pays particular attention to the security of their data, including their image.
 2. The agreement for educational services for a minor is concluded by their Guardian, who as a rule also exercises the related GDPR rights (Section X.3).
 3. The Controller processes minors' data only to the extent necessary to provide the educational service and to comply with the Act on Protecting Minors.
 4. Rules on capturing, processing and publishing the image of minor Participants, including the requirement of separate written Guardian consent, are set out in Section IV.1.4 of this Policy and Section 14 of the **Child Safeguarding Standards**, available on the Website and at the School's premises.
 5. Rules on the visibility of a minor Participant's results in the rewards system are set out in Section IV.6.4.
 6. Where an intervention procedure under the CSS is triggered, a minor's data (including, in justified cases, special categories of data such as health data) may be processed to the extent necessary to ensure their safety and disclosed to the competent authorities – the Police, the prosecutor's office, the family court or a social welfare centre – in accordance with the Controller's legal obligation.
 7. CSS procedure records are stored in a manner preventing access by unauthorised persons; access is limited to the Reporting and Support Coordinator and the Management Board.
-

XII. Security measures

The Controller applies technical and organisational measures appropriate to the risk, including: access control to systems and paper records, encryption of transmission (TLS) on the Website and Platform, two-factor authentication in key systems, confidentiality undertakings and processing authorisations for Employees and Associates, data-processing agreements with suppliers, and backups – to protect personal data against unauthorised access, loss or unlawful alteration.

XIII. Contact

1. For matters concerning personal data protection, please contact the Controller:
 - by e-mail: privacy@quasarhub.pl;
 - by post: QUASAR.HUB sp. z o.o., os. Stefana Batorego 79E/1, 60-687 Poznań, Poland;
 - by telephone: **+48 579 135 924**.
2. The Controller notes that the appointment of a formal Data Protection Officer is not mandatory under Art. 37 GDPR given the School's current scope of activity; the address above serves as the contact point for data protection matters until a DPO is appointed, if ever.

3. Reports concerning the safety of minors are directed to a separate address, som@quasarhub.pl, in accordance with Section 11 of the CSS.

XIV. Final provisions

1. This Policy is effective from **10 September 2026**.
2. Matters not governed by this Policy are subject to generally applicable law, in particular the GDPR and the Polish Personal Data Protection Act.
3. The Controller may amend this Policy, in particular where required by changes in the law, the development of the School's offering, or the deployment of new tools. The current version is always available on the Website, together with the date of its last update.
4. This Policy forms a coherent whole with the following documents:

DOCUMENT	SCOPE
Cookie Policy	details on Cookies (Section VII)
GDPR information notices	Art. 13 notices provided at the point of data collection
Child Safeguarding Standards + Annexes 1-6	protection of Participants under 18 (Section XI)
School Regulations and Terms of Sale (B2C)	§12 – personal data of Clients and Participants
Terms of Sale for Business Clients (B2B)	§12 – relationship of separate controllers
Polityka prywatności (PL)	the authoritative Polish original