

ROUTE2OPEN

Privacy and Cookie Notice

Version dated 8 September 2026

1. Who is responsible for your information?

ROUTE2OPEN sp. z o.o., ul. Austriacka 4, 64-100 Leszno, Poland, NIP 7831846387, KRS 0000932849 ("R2O", "we"), is the controller of the personal data it uses for its website, learning platform, training services, and community.

Contact us at info@route2open.com or write to our address above. This notice explains our processing under the EU General Data Protection Regulation (EU) 2016/679 (GDPR); reading it does not constitute general consent to process your data or marketing consent. It covers route2open.com, our learning platform, purchases, courses, bootcamps, materials, and communications. The provisions about the planned Discourse community apply once it becomes available.

2. What information do we receive, and from where?

We receive information when you create an account, order training, request materials, contact us or participate in courses and discussions: your name, email, account details, company, billing information, correspondence and requests, course allocations, access records, progress, quiz answers/results, and certificate records.

If your employer or a reseller purchases training for you, they may give us your name, email, and course allocation. We use these to arrange your access and contact you about the service. We identify the source and explain how we use the data at first contact, no later than one month after receiving it, or before disclosing it to another recipient if that happens sooner. We do not routinely send employers your learning progress or exam results.

We receive payment confirmations and transaction, refund, or dispute details from payment providers. Our systems also receive technical information such as IP addresses, device and browser information, access times, access logs, and security logs. If you choose Google sign-in, Google supplies the identity and profile information shown in its authorisation screen, particularly your email address and account identifier and, depending on the configuration, your display name, full name, or profile picture. We use these to create or recognise your account and enable sign-in. Removing the connection in Google does not, by itself, delete your R2O account.

Forms identify required information. Providing data necessary to enter into and perform the agreement is a condition of fulfilling an order or providing an account. Data required by tax or accounting law is mandatory to the extent specified by that law. Without other data needed for a specific purpose, such as verifying student eligibility, we may be unable to provide the relevant benefit. Additional information and marketing consent are optional. Marketing is not required for purchases, accounts, or free materials.

3. Why we use data

Purpose	Data and legal basis
Provide accounts, courses, bootcamps, included labs and requested downloads	Contact and account details, access records, progress, and assessment results: performance of our agreement with you, including a free account agreement, or steps you request before an agreement (Article 6(1)(b) GDPR).
Arrange company or reseller bookings	Participant and contact person details and business correspondence: our legitimate interests in delivering the purchased training and administering the business relationship (Article 6(1)(f) GDPR); performance of your subsequent individual account/service agreement where applicable (Article 6(1)(b) GDPR).
Process orders, payments, cancellations, complaints, and refunds; tax compliance and accounting	Order, payment and request information: performance of the agreement (Article 6(1)(b) GDPR). Billing and statutory records: compliance with tax, accounting, and other applicable legal duties (Article 6(1)(c) GDPR).
Verify student eligibility and issue certificates	Necessary evidence, assessment, and credential records: performance of the requested programme or certificate service (Article 6(1)(b) GDPR). Optional public certificate display: your consent (Article 6(1)(a) GDPR).
Operate the community and handle questions	Profile, posts, messages, and support correspondence: performance of the community or support service you request (Article 6(1)(b) GDPR). Moderation and other enquiries: our legitimate interests in a safe service and effective communication (Article 6(1)(f) GDPR).
Protect services and resolve disputes	Access logs and necessary documents, correspondence, or transaction evidence: our legitimate interests in security, preventing misuse and establishing, exercising, or defending claims (Article 6(1)(f) GDPR); legal duties where applicable (Article 6(1)(c) GDPR).
Send optional marketing or publish an agreed testimonial	Email preferences and consent records, or the testimonial and agreed attribution: your consent (Article 6(1)(a) GDPR). Electronic marketing also requires the permission described in section 6.
Use optional cookies and similar technologies	Device and activity information within the scope explained before you choose: your consent (Article 6(1)(a) GDPR). Necessary technical processing supports the requested service or our legitimate interest in security, under Article 6(1)(b) or (f) GDPR, as appropriate.

We send service messages, such as access instructions, password resets, scheduled training reminders, and material service changes, independently of marketing subscriptions.

4. Training, certificates, and community

Training. We do not record bootcamps. Your name or username, voice and contributions can be available to the trainer and other participants. Meeting messages and attendance information may

remain after the session according to the meeting settings. Do not share unnecessary personal data or confidential third-party information in exercises or labs.

Quizzes may be marked automatically against the course's answers and pass requirements; the result may determine whether a certificate is awarded. Contact us if you need a person to review a disputed result. We do not use these results to make employment, lending, or comparable decisions about you.

Student eligibility. Preferably use an institutional email address. If additional evidence is needed, provide only your name, institution, and the validity period of your current student status; cover unrelated identification numbers, date of birth and other unnecessary details. We delete document images after verification as described below.

Certificates. If you choose to make a certificate verifiable through a public link, the public record may include the holder's name, course, credential reference, issue/expiry information, and validity status. Anyone with the link can view it, including after you share it on LinkedIn. You may withdraw public display consent by contacting us; this does not, by itself, invalidate the certificate.

Community. We plan to provide a free community using Discourse software running on infrastructure managed by us or our hosting provider. These provisions apply once the community becomes available. Your username, optional profile information, posts, and uploads will be visible to the audience permitted to access the relevant part of the community. Private messages will be available to their participants; authorised administrators may access them when necessary for technical support, investigating abuse or legal duties. Activity notifications can be managed through the available account settings. Do not post other people's personal information without a lawful reason.

If we enable shared sign-in for the learning platform and community, we will link accounts using a user identifier and the information needed for sign-in and access, such as email address, username, and course-group permissions. The connection supports R2O services and does not constitute marketing consent.

We do not upload customer data into the generative AI tools used to produce course voices, avatars, or materials.

5. Who can receive your information?

Access is limited to people and organisations that need information for the purposes described here:

- **Training and technical staff:** R2O staff, authorised collaborators and selected STORDIS GmbH staff who help deliver training, support customers, or administer systems.
- **Service providers:** website, lab, and email hosting, maintenance, and backup providers; Zoho CRM; Microsoft services for Teams and business administration; accounting providers and relevant invoicing systems, including Microsoft Navision and retained historical Fakturownia records.

- **Payments, video and sign-in:** PayPal and Stripe handle payments; Vimeo supplies embedded video playback and receives technical information when its player connects; Google supplies the sign-in service if you choose it. These providers may process certain data as separate controllers for their own purposes under their privacy notices as well as providing services to us. Their roles depend on the activity; they are not all simply our processors.
- **Other recipients:** your chosen sign-in provider, recipients of your community contributions or public credentials, and competent authorities or professional advisers where a legal duty or necessary handling of a matter requires disclosure and there is an appropriate legal basis.

We use WordPress and Tutor LMS to operate our learning platform and manage accounts. Installing software, including self-hosted Discourse, does not by itself mean its developer receives your personal data. Providers processing data on our behalf act within the scope of that engagement. Authorised people may access data to the extent needed for their work.

Our relationship with STORDIS GmbH

STORDIS GmbH, Germany, is a separate group company. The Zoho CRM account used for R2O is contracted by STORDIS GmbH. Selected authorised personnel have access for technical support, administration, and training delivery. This support access does not give STORDIS permission to send its own marketing to all R2O contacts.

Where STORDIS resells our training, it is responsible for its sales relationship; R2O provides the learner account and training. Each company is responsible for the processing it determines for its own activities. Any separate marketing choice is described in section 6.

International processing

Some providers operate internationally, including in the United States and India. European hosting alone does not exclude overseas access. Transfers outside the European Economic Area (EEA) require an appropriate basis: an applicable European Commission adequacy decision or appropriate safeguards, such as standard contractual clauses with additional safeguards where necessary. You can ask us for the relevant recipient, country and a copy of the safeguards or information about where they are available.

Provider information: [Zoho](#), [Microsoft](#), [PayPal](#), [Stripe](#), [Vimeo](#), [Google](#).

6. Newsletter and separate STORDIS marketing

We send R2O newsletters and promotional emails only if you choose to receive them. Buying training, downloading a resource, creating an account, using Google sign-in, or accepting our service terms does not itself subscribe you. Delivery of requested materials is separate from consent to future promotional messages.

If we offer a separate STORDIS marketing choice and you give that consent, we may pass your email address and the evidence and scope of your choice to **STORDIS GmbH**, Ruebteile 24, 72574 Bad Urach, Germany, contact: info@stordis.com, so it can email you offers within that choice. STORDIS supplies its

own privacy information before you consent. We do not transfer your full learning history or student verification documents for this purpose.

Conversely, we use contact details received from STORDIS GmbH for R2O marketing only where your permission specifically covers R2O and that sharing. Existing consents concerning one company are not automatically extended to other group companies.

Each marketing email includes an unsubscribe option. You can also contact the sender directly. Withdrawing marketing permission does not cancel your course or account. Consent withdrawal affects future processing, not the lawfulness of processing before withdrawal. Public use of your testimonial with attribution is limited to the scope separately agreed with you.

7. How long we keep information

We separate operational data from records that must remain for another purpose. A legal retention duty does not justify keeping your entire learning profile indefinitely.

Information	Retention period or rule
Account, learning and access information	While necessary for your active account and service entitlements. After these end, only records still needed for certificates, legal duties or claims remain. Inactivity or a failed email delivery does not by itself cancel existing access rights.
Certificate record	The minimum record needed while the credential and its verification remain available, which can outlast course access and can be indefinite for a certificate with no expiry. Public display ends when you withdraw the relevant consent.
Student document images	Delete without undue delay after verification, and no later than 30 days after verification is completed. Retain only the necessary eligibility result, date and programme allocation while administering the programme, and afterwards only to the extent needed for a specific obligation or claim.
Enquiries that do not lead to a contract	Up to 12 months after the last meaningful contact about the matter, unless a specific dispute, legal duty or establishing, exercising, or defending claims requires relevant evidence longer.
Routine technical logs	Up to 90 days; relevant entries relating to an incident or claim may be isolated and kept longer, to the extent necessary, until the matter is resolved and the applicable claim limitation periods expire.
Orders, invoices, and dispute evidence	For applicable tax, accounting, and claim limitation periods. Polish tax records normally require five years from the end of the year in which tax payment was due; OSS records require ten years from the transaction year-end where that scheme applies. Suspension or interruption of the applicable period may extend relevant retention.

Information	Retention period or rule
Marketing information	Until withdrawal, the subscription ends or its purpose ceases. Afterwards, only minimal consent evidence and an unsubscribe/suppression record remain where needed to demonstrate compliance, honour your choice, or address claims.

We retain data needed for claims to the extent necessary until the applicable limitation period expires or, where proceedings are ongoing, until they are finally concluded and settled.

Deletion requests also cover a linked community account and personal information within posts, not only the username. Non-identifying discussion text may remain to preserve conversations. Replacing a username alone is not sufficient if the post's content still identifies the person.

Deleted data may remain temporarily in protected backups until overwritten through the applicable backup cycle. It is not used for ordinary business purposes. If a backup is restored, we apply the deletions already made. You can ask us about the backup period applying to your information.

8. Cookies and similar technologies

Cookies and local storage help a website remember information in your browser. Necessary technologies support functions you request, such as login, checkout, security and remembering your cookie choice. They do not require consent only to the extent covered by the statutory exception for transmitting a communication or providing a service expressly requested by the user.

Storing information on, or gaining access to information already stored on, your device is additionally governed by Article 399 of the Polish Electronic Communications Law of 12 July 2024 (Prawo komunikacji elektronicznej), which replaced Article 173 of the former Telecommunications Law of 16 July 2004 (Prawo telekomunikacyjne) and continues to implement the consent requirement of the ePrivacy Directive referred to above.

Optional analytics, advertising, and other non-essential technologies require your prior choice. You can accept, reject, or select individual purposes, and change or withdraw your choice through the mechanism provided for those technologies. Before you choose, we provide information about their actual purposes, providers, and operating periods. Continuing to browse is not consent. Rejecting optional tracking must not prevent access to a course you are entitled to use.

Embedded services such as Vimeo may receive your IP address and technical information when loaded, regardless of whether a cookie is stored. Necessary video delivery is distinguished from optional tracking; a privacy setting does not by itself mean that no information reaches the provider.

Browser settings can delete or block cookies but blocking necessary cookies may affect login or checkout. Choices are generally browser/device specific. External links, including social media links, take you to services with their own privacy information; following a link does not subscribe you to our marketing.

Withdrawing cookie consent is as easy as giving it: use the preference/consent management link available on every page to change or withdraw your choice at any time.

9. Your rights and changes to this notice

To the extent provided by the GDPR, you may request access and a copy, correction, erasure, restriction, and portability of your data. You may withdraw consent at any time. Where we rely on legitimate interests, you can object for reasons relating to your situation. **You can object to direct marketing at any time, without giving reasons.**

Email **info@route2open.com**. We may ask for proportionate information to confirm your identity. We normally respond within one month of receiving your request; if a lawful extension is necessary, we explain it within that month. Some records must remain for legal duties or claims even if you close an account.

You may complain to the President of Poland's Personal Data Protection Office (Prezes UODO), ul. Stanisława Moniuszki 1A, 00-014 Warsaw, uodo.gov.pl, or another competent supervisory authority.

We update this notice when our actual practices or legal duties change. We inform affected users of material changes as required, including before using data for a new purpose. An update does not create new marketing consent or change the terms of an earlier purchase.